# Avaya Video Conferencing Manager Deployment Guide

Issue 1
June 2010

© 2010 Avaya Inc.
All Rights Reserved.

### Notices

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

### Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

### Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

### Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

### Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, http://support.avaya.com/LicenseInfo ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone products or pre-installed on Hardware. "Hardware" means the standard hardware originally sold by Avaya and ultimately utilized by End User.

### License types

Designated System(s) License (DS). End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Shrinkwrap License (SR). Customer may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License"). (see "Third-party Components" for more information).

### Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil, offense under the applicable law.

### Third Party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright

### Preventing toll fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

### Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States

and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://support.avaya.com

Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

### Trademarks

**Avaya and Aura are trademarks of Avaya, Inc.**

Avaya is a registered trademark of Avaya Inc.

Avaya Aura is a trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

### Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: http://www.avaya.com/support

### Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

### Patent Notice

For patents covering LifeSize® products, refer to http://www.lifesize.com/support/legal.

## Welcome to Avaya Video Conferencing Manager

Avaya Video Conferencing Manager is a comprehensive management software solution for network administrators who manage video and voice communications systems in an IP environment. With Avaya Video Conferencing Manager, network administrators can do the following:

- Monitor and manage multi-vendor video and voice communications devices across the entire enterprise from a web browser. Avaya Video Conferencing Manager includes full-featured, standards-based video device management capabilities with real-time status and event notification.
- Manage and automate video and voice call scheduling. Enable call participants to schedule calls through Avaya Video Conferencing Manager using a central scheduling function, such as a help desk or video network operations center, or integrate Avaya Video Conferencing Manager with Microsoft Exchange Server to leverage existing information technology resources and enable users to schedule video and voice conferences using Microsoft Outlook.
- Generate reports for tracking inventory and analyzing device utilization and performance.

## About this Guide

This guide is for network administrators or anyone who manages video and voice communications systems in an IP environment and who needs to know how to install, upgrade, use, or maintain Avaya Video Conferencing Manager. Topics addressed in this guide include the following:

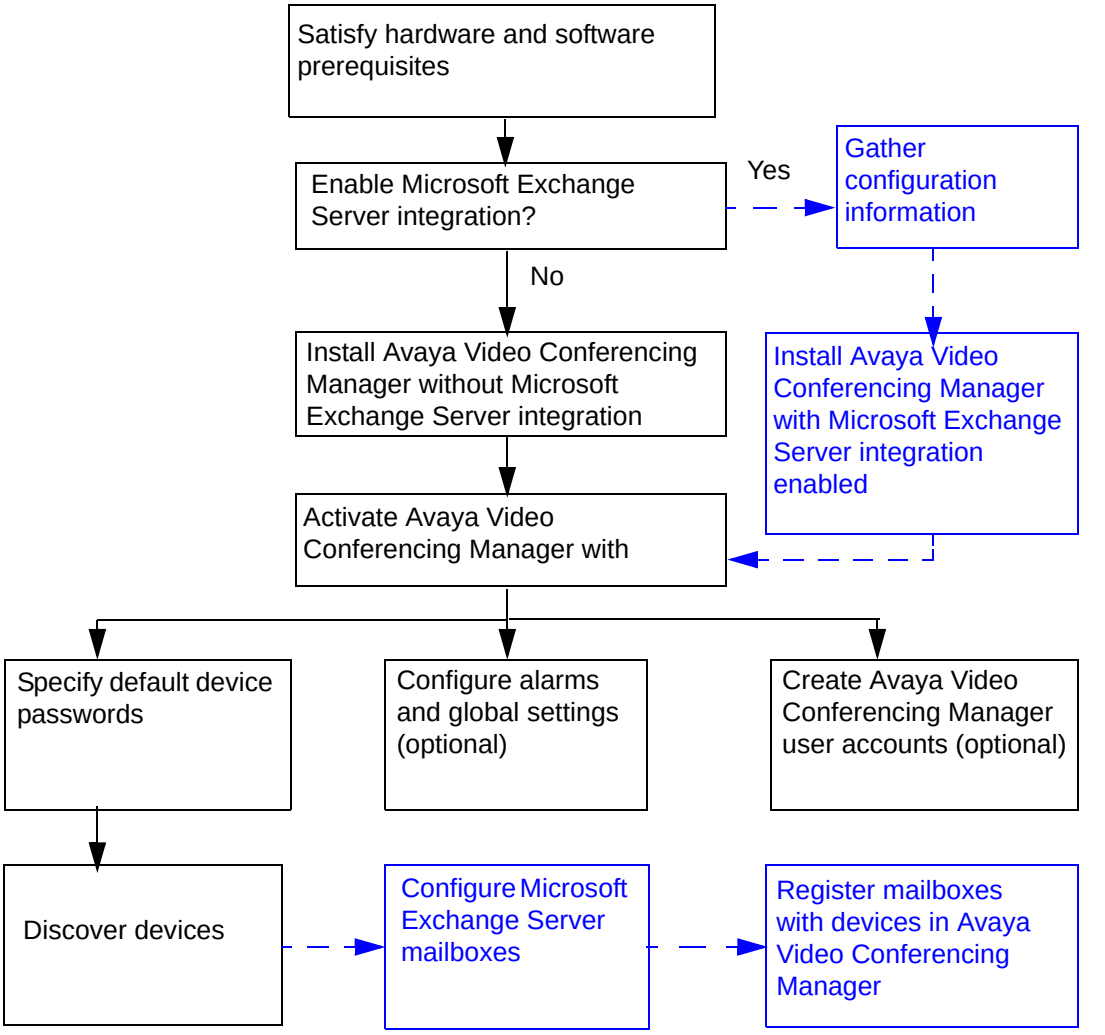
- planning an Avaya Video Conferencing Manager deployment
- planning to install Avaya Video Conferencing Manager software
- installing or upgrading Avaya Video Conferencing Manager
- configuring Avaya Video Conferencing Manager
- discovering and managing devices
- managing call scheduling
- generating reports
- using Avaya Video Conferencing Manager Administrator
- maintaining and troubleshooting an installation

## Preparing for an Avaya Video Conferencing Manager Deployment

Planning is essential to successfully deploying enterprise-level software solutions. To avoid unexpected problems and to stay on schedule, Avaya recommends a phased approach to deploying Avaya Video Conferencing Manager that includes planning, installing, testing, and training before going live. Use the information in this section to prepare an Avaya Video Conferencing Manager deployment plan for your organization.

## Deployment Overview

The following diagram shows the high-level tasks and associated dependencies involved in deploying Avaya Video Conferencing Manager for the first time. Use this diagram as a guide when preparing a schedule to include in your deployment plan. The tasks associated with Microsoft Exchange Server integration appear in blue with dotted line connectors. If you intend to integrate Microsoft Exchange Server with Avaya Video Conferencing Manager, you must enable the integration during installation of Avaya Video Conferencing Manager. You cannot enable the feature after installing Avaya Video Conferencing Manager.


Satisfy hardware and software prerequisites
Enable Microsoft Exchange Server integration?
Yes
Gather configuration information
No
Install Avaya Video Conferencing Manager without Microsoft Exchange Server integration
Install Avaya Video Conferencing Manager with Microsoft Exchange Server integration enabled
Activate Avaya Video Conferencing Manager with
Specify default device passwords
Configure alarms and global settings (optional)
Create Avaya Video Conferencing Manager user accounts (optional)
Discover devices
Configure Microsoft Exchange Server mailboxes
Register mailboxes with devices in Avaya Video Conferencing Manager

## Planning for Integration with Microsoft Exchange Server

The most important decision to make when planning an Avaya Video Conferencing Manager deployment is whether to enable Microsoft Exchange Server integration when you install Avaya Video Conferencing Manager. Avaya Video Conferencing Manager integrates with Microsoft Exchange Server 2003 or Microsoft Exchange Server 2007 to enable Microsoft Outlook users to schedule video or voice conference calls in Avaya Video Conferencing Manager without having an Avaya Video Conferencing Manager user account or knowledge about how to use Avaya Video Conferencing Manager. Without this feature, users of video and voice communications systems typically must call a help desk or similar scheduling facility to schedule a call through Avaya Video Conferencing Manager.

***Note:*** If you intend to integrate Microsoft Exchange Server with Avaya Video Conferencing Manager, you must enable the integration during installation of Avaya Video Conferencing Manager. You cannot enable the feature after installing Avaya Video Conferencing Manager.

In this release, enabling Microsoft Exchange Server integration also allows invitees to a video call scheduled through Microsoft Outlook to specify a video communications system through which they can be reached. To be included in the scheduled call, the device must be an external device that is not managed by Avaya Video Conferencing Manager. This enables invitees in your organization who are mobile, but who have access to video communications systems, and invitees external to your organization to include an external video communications device in a scheduled call. By default, this feature is disabled.

When you enable this feature, Avaya Video Conferencing Manager sends an email to all human participants that are included in the meeting invitation. The email lists the IP addresses of the video communications devices that are scheduled in the call and includes reply instructions. If a human participant wishes to participate through a video device that is not included in the scheduled call and not managed by Avaya Video Conferencing Manager, the participant can reply to the email with the command `call@`*`IPaddress`*, where *`IPaddress`* is the address of the external video communications device to use in the call.

Avaya Video Conferencing Manager then adds this device to the scheduled call and notifies the meeting organizer and all other human invitees of the change to the list of scheduled devices. If Avaya Video Conferencing Manager has no database entry for the device, it adds the device and its IP address to its database as an external device. The device then appears on the **Devices** page as an external device. For more information about external devices in Avaya Video Conferencing Manager refer to “Adding a New External Device” on page 48.

This feature also enables the meeting organizer to convert a video call from one that is placed automatically by Avaya Video Conferencing Manager to one that is placed manually by meeting participants. For more information about enabling and using this feature, refer to “Specifying a Preferred Method of Participation” on page 83.

***Caution:*** Enabling this feature allows a meeting invitee to add an external device to Avaya Video Conferencing Manager’s database without having a user account in Avaya Video Conferencing Manager. Avaya Video Conferencing Manager does not check the validity of the IP address of an external device that is added to a call through this mechanism. When the list of scheduled devices changes due to a reply from a human invitee to the email messages generated by this feature, all human invitees receive an email indicating the change. Avaya recommends that you use this feature in a test environment to ensure that it meets your needs before deploying it in your organization.

The Avaya Video Conferencing Manager installation program prompts you to choose a mechanism for authenticating Avaya Video Conferencing Manager users: either OpenLDAP (using the OpenLDAP server that installs with Avaya Video Conferencing Manager) or Active Directory.

***Note:*** If you choose to enable Microsoft Exchange Server integration, you must use Active Directory for user authentication in Avaya Video Conferencing Manager and the Active Directory server that you specify for user authentication, must be the same Active Directory server used by your Microsoft Exchange Server installation.

Integrating Microsoft Exchange Server with Avaya Video Conferencing Manager requires you to complete configuration tasks in both products. Ensure that your deployment plan includes coordinating configuration tasks with your Microsoft Exchange Server administrator and Active Directory administrator.

Enabling Microsoft Exchange Server integration is an optional step during the Avaya Video Conferencing Manager installation process. If you choose to enable this feature, you can disable it at any time after the installation process completes using configuration options in Avaya Video Conferencing Manager Administrator.

For more information about Avaya Video Conferencing Manager Administrator, refer to “Using Avaya Video Conferencing Manager Administrator” on page 88.

### Microsoft Exchange Server Integration Overview

Integrating Avaya Video Conferencing Manager with Microsoft Exchange Server includes the following tasks:

1. Create an email account in Microsoft Exchange Server for Avaya Video Conferencing Manager. This is the email account Avaya Video Conferencing Manager monitors to provide scheduling integration with Microsoft Exchange Server and Microsoft Outlook. Set the size of this mailbox to 500MB. Log into this account in Microsoft Outlook at least once to make it available for Avaya Video Conferencing Manager. While logged in, ensure the email box is set to the correct time zone.

   Avaya recommends that you set the archive interval for the Avaya Video Conferencing Manager mailbox to one week to prevent this mailbox from exceeding its storage limit.

   ***Caution:*** This email box must be dedicated for use by Avaya Video Conferencing Manager. Do not send general email to it or use it to send email. You must not open this email box or modify any email messages in it. Doing so will interfere with the integration of Microsoft Outlook scheduling with Avaya Video Conferencing Manager scheduling.

   Avaya Video Conferencing Manager supports only the Microsoft authentication protocol NT LAN Manager (NTLM). Avaya Video Conferencing Manager does not function properly if forms-based authentication is enabled in Microsoft Exchange Server 2003.

2. When the Avaya Video Conferencing Manager installation program prompts you to choose a mechanism for authenticating Avaya Video Conferencing Manager users, enter values for the **Configure for Active Directory** option. Ensure that the Active Directory server that you specify is the same one used by your Microsoft Exchange Server.

3. When prompted by the Avaya Video Conferencing Manager installation program to enable integration with Microsoft Exchange Server, be prepared to supply the following information:

   - If Microsoft Exchange Server requires HTTPS, select the corresponding check box.
   - The version of Microsoft Exchange Server (either Microsoft Exchange Server 2003 or Microsoft Exchange Server 2007) that you wish to integrate with Avaya Video Conferencing Manager.
   - Microsoft Exchange Server hostname or IP address. _____
   - Domain name for the server. _____
   - Avaya Video Conferencing Manager email address. This is the email address of the account described in task 1.

     _____

- Avaya Video Conferencing Manager email password. This is the password for the email account described in task 1.

4. After installing or upgrading Avaya Video Conferencing Manager, you can deploy the integration in one of the following ways. Refer to “Configuring Microsoft Exchange Server” on page 36 for detailed configuration steps for these options.

   **Option 1:**

   Create a resource mailbox in Microsoft Exchange Server for each conference room that contains a video or voice communications system managed by Avaya Video Conferencing Manager, if one does not already exist. Forward each conference room mailbox to the Avaya Video Conferencing Manager mailbox. In Avaya Video Conferencing Manager, associate the managed video or voice communications system with the email address of the mailbox resource for the conference room. When Microsoft Outlook users add conference rooms to a meeting request, Avaya Video Conferencing Manager automatically schedules the video or voice communications device associated with these conference rooms and places the call at the scheduled meeting time.

   ***Note:*** If your network includes MCUs managed by Avaya Video Conferencing Manager and you wish to allow meeting participants to select an MCU to include in a call scheduled through Microsoft Outlook, you must also create a resource mailbox in Microsoft Exchange Server for each MCU; forward each MCU mailbox to the Avaya Video Conferencing Manager mailbox; and associate the MCU with the email address of the mailbox resource for the MCU.

   **Benefits:**

   With this option, Microsoft Outlook users do not need to be aware of or add the video or voice communications devices to the meeting request as separate invitees. Avaya Video Conferencing Manager automatically places the scheduled call to the devices that reside in the conference rooms that the meeting organizer includes in the meeting request.

   **Limitations:**

   Users may not want to use video or voice communications devices in the meetings. Consider using this option if conference rooms that contain video or voice communications devices are dedicated for use as video or voice conferencing rooms. Users who wish to select an MCU to add to a call must remember to add the MCU as a separate invitee.

**Option 2:**

Create a resource mailbox in Microsoft Exchange Server for each video or voice communications system managed by Avaya Video Conferencing Manager. Forward each mailbox to the Avaya Video Conferencing Manager mailbox. In Avaya Video Conferencing Manager, associate the managed video or voice communications system with the email address of the mailbox resource. When Microsoft Outlook users create meeting requests, they add the conference rooms and the voice or video communications devices located in each room as separate invitees.

***Note:*** If your network includes MCUs managed by Avaya Video Conferencing Manager and you wish to allow meeting participants to select an MCU in a call scheduled through Microsoft Outlook, you must also create a resource mailbox in Microsoft Exchange Server for each MCU; forward each MCU mailbox to the Avaya Video Conferencing Manager mailbox; and associate the MCU with the email address of the mailbox resource for the MCU.

**Benefits:**

Microsoft Outlook users can create meeting requests with or without voice or video communications devices as invitees.

**Limitations:**

Microsoft Outlook users who want to use video or voice communications devices must include both the conference rooms and the video or voice communications devices as invitees to schedule calls.

Scheduling devices for a conference call in Avaya Video Conferencing Manager does not prevent the conference rooms that contain these devices from being reserved for the same meeting time by another meeting organizer in Microsoft Outlook.

## Preparing Your Environment

Whether you are installing Avaya Video Conferencing Manager for the first time or upgrading from a previous release, ensure that your environment meets the hardware and software prerequisites, including port access and client support requirements, in “Planning to Install Avaya Video Conferencing Manager Software” on page 14.

## Gathering Device Usernames and Passwords

After you install Avaya Video Conferencing Manager, you can use it to discover and manage supported devices. When Avaya Video Conferencing Manager attempts to manage a device, it logs on to the device’s command line or administrative interface using the logon information that you supply for each make of supported device in the **Passwords** page. If the logon information is missing in the **Passwords** page, or has changed on the device, you must manually update the login information on each discovered device in Avaya Video Conferencing Manager before Avaya Video Conferencing Manager can manage it. Before you discover devices, gather logon information for the devices that you intend to manage with Avaya Video Conferencing Manager. For more information, refer to “Specifying Default Passwords for Device Management” on page 30.

## Planning for Users

Avaya Video Conferencing Manager supports multiple users and controls user access to functionality through the use of roles. After you install Avaya Video Conferencing Manager you can add users. Review the information about user roles and accounts in “Managing User Accounts” on page 40 to determine which users to add and roles to assign. “Appendix A: User Role Access” on page 101 identifies the access level by role for each task that users can perform in Avaya Video Conferencing Manager.

## Configuring Alarms

Avaya Video Conferencing Manager includes hundreds of alarms that span 15 categories. Before training users to monitor and respond to alarms, Avaya recommends that you determine which alarms you wish to monitor. Refer to “Appendix B: Alarms by Category” on page 106 for a complete list of alarms, including each alarm’s description and default status. After you install Avaya Video Conferencing Manager, set the monitoring status of the alarms that you wish to monitor to **ON** and the status of all others to **OFF** on the **Alarms Configuration** page in Avaya Video Conferencing Manager Administrator.

You can also forward traps from all managed video and voice communications devices to third party monitoring systems using the **Northbound Settings** page in Avaya Video Conferencing Manager Administrator or on a device-specific basis using the **Northbound** tab in the **Device details** page for a single device. For more information refer to “Using Avaya Video Conferencing Manager Administrator” on page 88 and “Forwarding SNMP Traps with Northbound Settings” on page 53.

## Configuring Global Settings

Avaya Video Conferencing Manager Administrator enables you to set configuration options that affect how certain features work in Avaya Video Conferencing Manager and to disable or re-enable Microsoft Exchange Server integration and associated options. Review the information about this tool in “Using Avaya Video Conferencing Manager Administrator” on page 88 to determine which configuration options you wish to change for your environment. Avaya recommends that you configure these options before training users.

## Developing a Test Environment and Plan

Avaya recommends that you create a test environment for learning how to use Avaya Video Conferencing Manager, testing new features, and training new users. For example, after you install Avaya Video Conferencing Manager, discover a few devices at a time in a very limited IP address range or use a specific IP address to add a limited number of a variety of devices to use as test devices for device management and call scheduling tasks. Isolate or limit access to these devices. Use the device management and call scheduling procedures in this guide to create a test plan.

If you plan to enable Microsoft Exchange Server integration, be sure to include call scheduling through Microsoft Outlook as part of the test plan for these devices. Use the information in “Scheduling Conferences in Microsoft Outlook” on page 80 and, if you plan to enable it, “Specifying a Preferred Method of Participation” on page 83.

### Developing a Training Plan

Use the procedures in this manual and information about user roles to assist you in developing a training plan and training materials customized to your environment. If you enabled Microsoft Exchange Server integration with your installation, both Avaya Video Conferencing Manager users and Microsoft Outlook users will need to know how to schedule video and voice calls through Microsoft Outlook. Refer to “Scheduling Conferences in Microsoft Outlook” on page 80 and, if you plan to enable it, “Specifying a Preferred Method of Participation” on page 83.

If you installed Avaya Video Conferencing Manager without enabling Microsoft Exchange Server integration, and plan to use it for call scheduling, you may need to establish a training plan for users who staff a centralized scheduling function, such as a help desk or video network operations center, and procedures for meeting participants who wish to use a centralized scheduling service.

### Planning for Reports

Examine the reports available in Avaya Video Conferencing Manager to determine which ones you want to generate and how often. Avaya Video Conferencing Manager includes a reports subscription feature that automates report generation and delivery. For more information, refer to “Generating Reports” on page 86.

### Planning for Maintenance

After you install and configure Avaya Video Conferencing Manager and discover devices, Avaya recommends that you back up your installation. For more information about backing up the Avaya Video Conferencing Manager database, refer to “Database Management” on page 89. If you plan to enable Microsoft Exchange Server integration, be sure to read “Maintenance with Microsoft Exchange Server Integration” on page 96.

## Planning to Install Avaya Video Conferencing Manager Software

Before you install Avaya Video Conferencing Manager, ensure that your environment meets the following requirements.

> ***Caution:*** If you are upgrading from a previous release, refer to “Upgrading Avaya Video Conferencing Manager” on page 25 for important information about upgrade prerequisites.

If you plan to delay the installation after completing hardware and software prerequisite tasks, consider securing the hardware or restricting access to it to prevent use that may interfere with the installation process or cause the installation to fail.

## Hardware

Avaya Video Conferencing Manager supports the following minimum server configuration:

- 2.4GHz Pentium 4 processor
- 1GB RAM
- At least 500MB of free hard disk drive space (Avaya recommends 4GB)

  ***Note:*** Dual NIC cards are not supported on the Avaya Video Conferencing Manager server.

## Software

Ensure that the following software is installed on the server before you install Avaya Video Conferencing Manager:

- Microsoft Windows Server 2003 with Service Pack 1 (minimum) or Service Pack 2 (recommended)
- You must install and activate the following Windows components on the server. Refer to “Installing Windows Components” on page 20 for information about installing these components:
  - Application Server Console
  - ASP.NET
  - Enable Network COM+ Access
  - Enable Network DTC Access
  - Internet Information Server (IIS) v6.0 or later
- If you intend to use SSL to access Avaya Video Conferencing Manager from a web client, ensure that you obtain a valid server certificate.

Avaya Video Conferencing Manager is not supported on a server with an Active Directory installation or that is a domain controller. Ensure that Active Directory is not installed on the server on which you intend to install Avaya Video Conferencing Manager and that the server is not a domain controller.

The Avaya Video Conferencing Manager installation program installs an OpenLDAP server, the Microsoft .NET Framework 2.0 if not already installed, and PostgreSQL v8.3. You must be logged in as a user with administrator privileges to install these programs. Before you run the installation program, ensure that the following prerequisites are met on the computer on which you intend to install Avaya Video Conferencing Manager:

- You have administrator rights to install the applications.
- An existing OpenLDAP installation does not exist.
- An existing PostgreSQL installation does not exist.
- If OpenSSL exists on the server, ensure that the version is 0.9.7 or later or delete the LIBEAY32.dll and SSLEAY32.dll files (located in the `C:\windows\system32` folder). The Avaya Video Conferencing Manager installation program installs a compatible version of these files if OpenSSL does not exist on the server. If the Avaya Video Conferencing Manager installation program detects an earlier version, an error message appears indicating that you must delete the LIBEAY32.dll and SSLEAY32.dll files. When you click **OK** in the message dialog box and then click **Next** in the installation dialog box, the installation program quits. You must then delete the LIBEAY32.dll and SSLEAY32.dll files and uninstall Avaya Video Conferencing Manager before running the Avaya Video Conferencing Manager installation program again. To uninstall Avaya Video Conferencing Manager, refer to “Removing Avaya Video Conferencing Manager” on page 99.

  ***Caution:*** If you are performing an upgrade and the Avaya Video Conferencing Manager installation program encounters an incompatible existing version of OpenSSL, uninstalling Avaya Video Conferencing Manager removes the installation. You cannot continue the upgrade or return your existing Avaya Video Conferencing Manager installation to its previous state without uninstalling Avaya Video Conferencing Manager, reinstalling the previous version and restoring its database from a backup. If you are planning to upgrade your Avaya Video Conferencing Manager installation, ensure that you check for an existing OpenSSL installation before performing the upgrade. For more information about upgrade prerequisites, refer to “Upgrading Avaya Video Conferencing Manager” on page 25.

## Client Support

You can access the Avaya Video Conferencing Manager user interface from a computer equipped with the following:

- A supported web browser (refer to the Release Notes at support.avaya.com)
- 256MB memory
- Adobe Flash Player (refer to the Release Notes at support.avaya.com for supported versions)

  ***Note:*** Adobe Flash Player is included with the Avaya Video Conferencing Manager installation program as an optional installation step, or you can download it directly from www.adobe.com.

## Ports

The Avaya Video Conferencing Manager installation program automatically installs and prompts you to configure an OpenLDAP server. The OpenLDAP server installs on the same server as the Avaya Video Conferencing Manager software and uses TCP port 389 by default. You can accept the default port if not already in use, or specify a different port for the server to use. Ensure that any firewalls that are installed on the Avaya Video Conferencing Manager server are configured to allow incoming traffic on this port.

Avaya Video Conferencing Manager is based on Microsoft's .NET framework and uses TCP port 8085 for IIS to Avaya's server communication.

Avaya Video Conferencing Manager uses TCP port 3336 when scheduling conferences through Radvision and MCUs.

The user interface is hosted on IIS on a Microsoft Windows Server 2003 platform on port 80, or port 443 if the SSL option is used. Dynamic updates are provided through TCP and UDP port 4296 of the web server.

Avaya Video Conferencing Manager also requires TCP port 483 for Adobe Flash security. Adobe Flash clients retrieve a master policy file from this port on the server.

Avaya Video Conferencing Manager supports management of video communications devices through standard APIs such as those listed in the following table. Communication with these devices is through default ports provided for FTP, SNMP, and HTTP.

| Protocol | Ports |
|---|---|
| FTP | TCP port 21 for outbound communication from Avaya Video Conferencing Manager to Codian, Tandberg, and Polycom devices |
| Telnet | TCP port 23 for outbound communication from Avaya Video Conferencing Manager to Tandberg devices<br>TCP port 24 for outbound communication from Avaya Video Conferencing Manager to Polycom devices |
| SSH | TCP port 22 outbound communication from Avaya Video Conferencing Manager |
| SNMP v1, v3 | UDP port 161 for inbound communication<br>Avaya Video Conferencing Manager connects to this port on a device to retrieve data from the device.<br>UDP port 162<br>Avaya Video Conferencing Manager listens on this port to receive traps from a device. When the device needs to forward a trap, it connects to the Avaya Video Conferencing Manager server on this port to deliver the trap. |
| HTTP | TCP and UDP port 80 |
| HTTPS | TCP port 443 |
| LDAP | TCP port 389 for OpenLDAP (unless changed during installation) for inbound communication from Avaya devices to the Avaya Video Conferencing Manager server |

## Data Storage

Avaya Video Conferencing Manager stores data in the PostgreSQL database management system. The installation program installs PostgreSQL on the same server as Avaya Video Conferencing Manager.

A database instance is created using Trusted Windows Authentication. The connection mechanism uses the PostgreSQL Data Provider. Avaya Video Conferencing Manager uses an LDAP-based H.350 compliant address book.

## Installing Avaya Video Conferencing Manager

Before installing Avaya Video Conferencing Manager, ensure that your environment meets all hardware and software requirements described in “Planning to Install Avaya Video Conferencing Manager Software” on page 14. If you intend to enable and configure Microsoft Exchange Server integration with your Avaya Video Conferencing Manager installation, ensure that you have read and understand the requirements for enabling and configuring this feature as described in “Preparing for an Avaya Video Conferencing Manager Deployment” on page 5 and collected the information required to enable this feature during the installation process.

> ***Caution:*** If you are upgrading from a previous release, refer to “Upgrading Avaya Video Conferencing Manager” on page 25 for important information about upgrade prerequisites.

Installing Avaya Video Conferencing Manager includes the following tasks:

- Install Microsoft Windows components.
- Run the Avaya Video Conferencing Manager installation program.

If you are upgrading from a previous release, complete the steps in “Upgrade Prerequisites” on page 25.

The Avaya Video Conferencing Manager installation program also installs Avaya Video Conferencing Manager Administrator, a web-based tool you can use to view and change the status of services and modify application, alarm, OpenLDAP, email, Microsoft Exchange, conference, database management (backup and restore), license, and report configuration settings. For more information, refer to “Using Avaya Video Conferencing Manager Administrator” on page 88.

## Installing Windows Components

Before installing Avaya Video Conferencing Manager, you must install the following Microsoft Windows components on the server:

- Application Server Console
- ASP.NET
- Enable Network COM+ Access
- Enable Network DTC Access
- Internet Information Server (IIS)

To install the Microsoft Windows components, follow these steps:

1. From the Windows **Control Panel**, choose **Add or Remove Programs** and click **Add/Remove Windows Components** in the left panel.
2. From the **Windows Components Wizard**, select **Application Server** and click **Details**.
3. Enable the following required subcomponents:
   - **Application Server Console**—Provides a central location from which to administer web applications.
   - **ASP.NET**—Required to deploy ASP.NET web applications to a production server. Avaya Video Conferencing Manager is an ASP.NET web application.
   - **Enable Network COM+ Access**—Builds on Component Object Model (COM) integrated services and features. Most Avaya Video Conferencing Manager components are service components.
   - **Enable Network DTC Access**—Coordinates COM+ transactions. Avaya Video Conferencing Manager components use DTC for remote calls.
   - **Internet Information Server (IIS)**—Provides the infrastructure for .NET and existing web applications and services. The default enabled subcomponents **Internet Information Service Manager** and **World Wide Web Service** are required to run Avaya Video Conferencing Manager.
4. Click **OK**.
5. Click **Next** to complete the installation.
6. Close the **Add or Remove Programs** window.

## Running the Installation Program

The Avaya Video Conferencing Manager installation program installs and prompts you to configure the Avaya Video Conferencing Manager software and an OpenLDAP server. Avaya recommends that you collect the following required information before performing the installation:

- fully qualified domain name of your organization's SMTP server
- email address of the person who will receive Avaya Video Conferencing Manager alarms
- IP address for the OpenLDAP server
- port for the OpenLDAP server (the default is port 389)
- domain suffix of the OpenLDAP directory tree structure (for example, *example.com*)
- If enabling Microsoft Exchange Server integration:
  - Microsoft Exchange server's IP address
  - domain name for the Microsoft Exchange server
- IP address for the Avaya Video Conferencing Manager server

To run the Avaya Video Conferencing Manager installation program, follow these steps:

1. If the **Welcome** screen does not appear after you insert the distribution media, open the Avaya Video Conferencing Manager distribution media, and double-click **setup.exe**.
   a. Click **Next** on the **Welcome** screen.
   b. Accept the terms of the license agreement and click **Next**.
   c. Complete the **Customer Information** screen and click **Next**.

      You can specify whether you want to install Avaya Video Conferencing Manager only for yourself or for all users of the server.
   d. Select **Typical** to install Avaya Video Conferencing Manager in the default location (`Program Files\Avaya\SystemManager`) or select **Custom** to identify a directory into which to install Avaya Video Conferencing Manager.
   e. Click **Next**, then click **Install** to begin the installation.

      When this stage of installation is complete, the **Avaya Video Conferencing Manager Configuration** screen appears.

2. To configure Avaya Video Conferencing Manager, enter values for the following fields.

   ***Note:*** The SMTP server and email addresses are required for alerts.

   a. **SMTP Server**—Enter the fully qualified domain name of the SMTP server for your organization.

   b. **To Email Address**—Enter the email address of the recipient who will receive alerts.

   c. **From Email Address**—Enter the email address that will appear as the *From* address of an alert message.

      For example: Avaya_Video_Conferencing_Manager@example.com)

   d. **Use https**—Specify whether to use SSL for communication between the Avaya Video Conferencing Manager server and the web clients or to use HTTP.

   e. **Make Avaya Video Conferencing Manager the default web site?**—Choose **Yes** for the server's host name to be an alias for the Avaya Video Conferencing Manager URL. Users can enter this host name in their browsers to access Avaya Video Conferencing Manager, for example:

      `http://<hostname>`

   f. Click **Next**.

      The **OpenLDAP Installation** dialog box appears and prompts you to continue. OpenLDAP installs on the same server as Avaya Video Conferencing Manager and is a required component of an Avaya Video Conferencing Manager installation.

3. Click **Next** to continue.

   The setup program installs the OpenLDAP server. The **LDAP Configuration** dialog box appears.

4. Complete the LDAP server configuration by entering values in the following fields:

   a. In the **OpenLDAP Settings** area, complete the following:

      - From the **OpenLDAP Server IP** list, select the IP address for the OpenLDAP server. OpenLDAP installs on the same server as Avaya Video Conferencing Manager.
      - Specify a **Port** to use. The default is port 389.
      - Specify the **domain suffix** for the OpenLDAP directory tree structure. For example, *example.com*.

   b. In the **User Authentication** area, select and enter values in the fields for one of the following:

      ***Note:*** If you plan to enable and configure the Microsoft Exchange Server integration feature, you must use Active Directory for user authentication in Avaya Video Conferencing Manager. The Active Directory server specified in this step must be the same one used by your Microsoft Exchange Server.

      - **Configure for OpenLDAP**—Create a user account for logging into Avaya Video Conferencing Manager. Enter a user name and password.

      - or -

      - **Configure for Active Directory**—Specify an existing domain and an existing user account for logging into Avaya Video Conferencing Manager. The specified user must be set up so that passwords never expire. Avaya Video Conferencing Manager uses Active Directory to access the user accounts for authentication purposes only, and does not add, delete, or modify user accounts.

        The machine on which you are installing Avaya Video Conferencing Manager must already be on the domain if you choose this option.

   ***Note:*** The user must have administrator privileges. The password is case-sensitive.

   c. Click **Configure LDAP**.

      When the configuration completes, a status message appears.

   d. Click **OK** to close the status message.

   The **Avaya Video Conferencing Manager configuration for Microsoft Exchange support** dialog box appears.

5. By default, **Enable Exchange server integration with Avaya Video Conferencing Manager** is selected. Complete the following fields:
   - If your Microsoft Exchange Server requires HTTPS access, select the **Exchange server requires HTTPS access** check box.
   - Click either **Exchange 2003** or **Exchange 2007** to specify which version of Microsoft Exchange Server you wish to integrate with Avaya Video Conferencing Manager.
   - Enter the Microsoft Exchange Server's IP address in **Exchange Server address**.
   - Enter the domain name for the Microsoft Exchange Server in **Domain Name**.
   - Enter an email address for **Avaya Video Conferencing Manager email address**. For example, Avaya_Video_Conferencing_Manager@example.com. This is the email account Avaya Video Conferencing Manager monitors to provide scheduling integration with Microsoft Exchange Server.

     ***Caution:*** This email box must be dedicated for use by Avaya Video Conferencing Manager. Do not send general email to it or use it to send email. You must not open this email box or modify any email messages in it. Doing so will interfere with the integration of Microsoft Outlook scheduling with Avaya Video Conferencing Manager scheduling. Additionally, set the size of this mailbox to 500MB. You must log on to the account in Microsoft Outlook at least once to make it available for Avaya Video Conferencing Manager. While logged in, ensure the email box is set to the correct time zone.
   - Enter a password for the Avaya Video Conferencing Manager email box in **Avaya Video Conferencing Manager password**.
6. Click **Next**.

   The **Server Location Configuration** dialog box appears.
7. Select values for the following fields:
   - From the **Country** list, select the country in which the Avaya Video Conferencing Manager server is located.
   - From the **State** list, select the state in which the Avaya Video Conferencing Manager server is located, if applicable.
   - From the **Server IP Address** list, select the IP address for the Avaya Video Conferencing Manager server.

8. Click **Configure** and then click **OK**.

   ***Note:*** If the installation fails, refer to “Troubleshooting Avaya Video Conferencing Manager” on page 95. If you must reinstall Avaya Video Conferencing Manager after fixing the problem, ensure that you uninstall the OpenLDAP server and the PostgreSQL database before attempting to install again. Refer to “Removing Avaya Video Conferencing Manager” on page 99.

9. Click **Finish**.

   The Avaya Video Conferencing Manager installation is complete.

10. Restart your computer to ensure that the changes take effect.

# Upgrading Avaya Video Conferencing Manager

The Avaya Video Conferencing Manager installation program installs the Microsoft .NET Framework 2.0 if not already installed. During an upgrade, the Avaya Video Conferencing Manager installation program changes the ASP.NET version of all web sites installed in IIS to v2.0. Other web sites installed in IIS that are not running in their own application pools may not function properly after the upgrade. To work around this issue after performing the upgrade, refer to “Installation Ends with an Error Message” on page 96.

## Upgrade Prerequisites

Before you upgrade your Avaya Video Conferencing Manager installation, complete the following tasks:

- Avaya recommends that you back up your Avaya Video Conferencing Manager database before performing an upgrade. Refer to the product documentation for the version of Avaya Video Conferencing Manager from which you are upgrading for backup instructions.
- Create a backup copy of the SharedXML folder and the *.config files that are located in the installation folder.
- Ensure that the server on which Avaya Video Conferencing Manager is installed has at least 500MB of free disk space.
- Ensure that the server on which Avaya Video Conferencing Manager is installed does not have an Active Directory installation and is not a domain controller.
- Ensure that you have administrator rights to perform the upgrade.
- Ensure that Avaya Video Conferencing Manager is not in use during the upgrade.

- If OpenSSL exists on the server, ensure that the version is 0.9.7 or later or delete the LIBEAY32.dll and SSLEAY32.dll files (located in the C:\windows\system32 folder). The Avaya Video Conferencing Manager installation program installs a compatible version of these files if OpenSSL does not exist on the server.

  ***Caution:*** If the Avaya Video Conferencing Manager installation program detects an earlier version of OpenSSL, an error message appears indicating that you must delete the LIBEAY32.dll and SSLEAY32.dll files. When you click **OK** in the message dialog box and then click **Next** in the installation dialog box, the installation program quits. You must then delete the LIBEAY32.dll and SSLEAY32.dll files and uninstall Avaya Video Conferencing Manager using the steps in “Removing Avaya Video Conferencing Manager” on page 99. You cannot continue the upgrade or return your existing Avaya Video Conferencing Manager installation to its previous state without uninstalling Avaya Video Conferencing Manager, reinstalling the previous version and restoring its database from a backup. If you are upgrading your Avaya Video Conferencing Manager installation, ensure you do not have an incompatible version of OpenSSL on the computer on which Avaya Video Conferencing Manager is installed before you perform the upgrade.

## Performing an Upgrade

Before performing an upgrade, ensure that you complete all tasks in “Upgrade Prerequisites” on page 25.

To upgrade from a previous version of Avaya Video Conferencing Manager, follow these steps:

1. On the Avaya Video Conferencing Manager distribution media, double-click **setup.exe**. The program automatically detects an existing Avaya Video Conferencing Manager installation that is eligible for an upgrade.
2. When prompted to continue with the upgrade, click **Next**.
3. Click **Next**.
4. Click **Finish**.
5. Restart your server to ensure that the changes take effect.

***Note:*** To integrate Microsoft Exchange/Outlook scheduling with Avaya Video Conferencing Manager, refer to the instructions in “Configuring Microsoft Exchange Server” on page 36.

# Configuring Your Environment

After installing Avaya Video Conferencing Manager, configure your environment by completing the following tasks:

- Access Avaya Video Conferencing Manager from your web browser.
- Activate Avaya Video Conferencing Manager with a license key.
- Specify default passwords for device management.
- Discover the devices on your network.
- Familiarize yourself with the Avaya Video Conferencing Manager Dashboard.
- If you chose to integrate Microsoft Outlook with Avaya Video Conferencing Manager during installation, configure both products to complete the integration.
- Create user accounts (optional).
- Configure alarms and other global settings (optional).

## Accessing Avaya Video Conferencing Manager

After installing Avaya Video Conferencing Manager on a server, you can access the user interface from a supported web browser.

To log in the first time, follow these steps:

1. Access the user interface by entering the URL in your web browser, for example:

   ```
   http://<hostname>
   ```

   ***Note:*** If Avaya Video Conferencing Manager is not configured to be the default web site for the server, you must enter the full path for Avaya Video Conferencing Manager, for example:

   ```
   http://<hostname>/avayasystemmanager
   ```

2. If Avaya Video Conferencing Manager detects an incompatible version of Adobe Flash Player or Adobe Flash Player is not installed on your system, a page appears that contains links to installation files for a supported version. Install the software, close your browser, and repeat step 1. The Avaya Video Conferencing Manager launch page appears.

   ***Note:*** If the launch page does not appear, refer to “Troubleshooting Avaya Video Conferencing Manager” on page 95.

3. Select a language and click **Launch Avaya Video Conferencing Manager**.

   The Avaya Video Conferencing Manager login screen appears.

4. Enter a **User name** and **Password**. These values are the user name and password that you entered for user authentication in step 4 on page 23.

   ***Note:*** If cookies are enabled on your browser, Avaya Video Conferencing Manager remembers the user name and password for subsequent sessions if you select the **Remember me** check box.

5. Press the **Enter** key or click the **LOGIN** button. The Avaya Video Conferencing Manager Dashboard appears.

   After logging in as a user with administrator privileges, you can set up other users. Refer to “Managing User Accounts” on page 40.

## Obtaining the License Key

To use Avaya Video Conferencing Manager, you must configure the software with a license key (located on the Avaya Video Conferencing Manager CD packaging) and activate the software. Contact your Avaya reseller or Avaya Technical Services if you do not have a license key and need assistance.

***Note:*** Once you have activated the license key with your software, you cannot reuse that key.

### Activating Avaya Video Conferencing Manager through the Internet

To activate Avaya Video Conferencing Manager automatically using the Internet, follow these steps:

1. Access Avaya Video Conferencing Manager.
2. A row of icons at the bottom of the Avaya Video Conferencing Manager Dashboard serves as a navigation bar. Click the **License Manager** icon.
3. In the **License key** section, enter the license key included with the Avaya Video Conferencing Manager CD packaging.
4. Click **Save**.

   Avaya Video Conferencing Manager automatically contacts the License Key server and unlocks the software. The **License Details** section of the License Manager shows the number of seats and the type of license (demo version or purchased version), the total number of licenses in use, and the number remaining. The total number of licenses in use and the number remaining also appear in the **Device Inventory** section of the Avaya Video Conferencing Manager Dashboard.

### Activating Avaya Video Conferencing Manager without Internet Access

To activate Avaya Video Conferencing Manager manually without Internet access, follow these steps:

1. Call the Avaya Video Technical Center at 800-242-2121 extension 15626 requesting an unlock key for your license key.
   The following information is required:
   - Customer name
   - Sold to or Functional location
   - Purchase Order number
   - MAC address
   - License key
   - Channel Partner or reseller (if applicable)
2. Access Avaya Video Conferencing Manager.
3. In the navigation bar, click the **License Manager** icon.
4. In the **Unlock key** section, enter the license key included with the Avaya Video Conferencing Manager CD.
5. Enter the unlock key provided to you through email from Avaya.
6. Click **Save**.

   Avaya Video Conferencing Manager unlocks the software with the key information you provided. The **License Details** section of the License Manager shows the number of seats and the type of license (demo version or purchased version), the total number of licenses in use, and the number remaining. The total number of licenses in use and the number remaining also appear in the **Device Inventory** section of the Avaya Video Conferencing Manager Dashboard.

## Specifying Default Passwords for Device Management

When Avaya Video Conferencing Manager attempts to manage devices, it uses the device logon information that you specify for each make of supported third-party device in the **Password** page.

***Note:*** Avaya Video Conferencing Manager automatically uses the default command line interface user (auto) and password (avaya) when attempting to manage Avaya devices.

If you do not specify a valid user name and password for supported third-party devices, or if the password that you specify has been changed on a device, the devices appear on the **Devices** page with a **Login failed** icon in the **Status** column and you cannot manage them until you update the password for each device.

***Note:*** Updating a password for a device in Avaya Video Conferencing Manager changes the password stored for that device in the Avaya Video Conferencing Manager database. It does not change the password stored on the device. To change the password stored on the device using Avaya Video Conferencing Manager, the device must be managed in Avaya Video Conferencing Manager. When you use Avaya Video Conferencing Manager to change a password on a managed device, the password is automatically updated in the Avaya Video Conferencing Manager database. For more information about updating or changing device passwords using Avaya Video Conferencing Manager, refer to “Managing Device Passwords” on page 58.

To enter default user names and passwords to use for discovering devices, follow these steps:

1. Access Avaya Video Conferencing Manager.
2. In the navigation bar, click the **Password** icon.
3. In the **Other Protocols** section, select the make of the third party device for which you wish to enter a user name and password. Refer to the documentation that accompanies your third party devices for information about the device’s default user name and password. Avaya Video Conferencing Manager supports only one user name and password for each make of supported device as the default to use during device discovery.
4. Click **Add**.

By default, Avaya Video Conferencing Manager uses SNMP to show detailed information about a discovered device, such as its make, model, and software version. The community string is a password used to access the device when you are sending SNMP traps. If the community string is correct, the device responds with the requested information. If the community string is incorrect, the device simply discards the request and does not respond. The default value of the community string is `public`. To change the default value, follow these steps:

1. Click the **Password** icon on the navigation bar.
2. In the section that pertains to the SNMP version that you use on your network, select the make of the third party device.
3. Enter a value for **Community String** for SNMP v1 or v2, or enter a **Username** for SNMP v3 or other protocols.
4. Click **Add**.

## Discovering Devices

After you configure default passwords for device management, follow these steps to discover and begin managing devices in Avaya Video Conferencing Manager:

1. Access Avaya Video Conferencing Manager.
2. In the navigation bar, click the **Devices** icon.
3. Click **Discover devices** on the **Actions** list and then click **Submit**.
4. Discover a single device or discover devices in a range of IP addresses.
   - To discover a single device, choose **Single IP** in the **Search By** list. Enter the IP address in the **IP Address** box.
   - To discover devices in a range of IP addresses, choose **IP Range** in the **Search By** list. Enter the IP address range in the **From** and **To** boxes.

   ***Note:*** When entering a large range of IP addresses, a delay may occur due to network latency. However, you can continue to interact with the Avaya Video Conferencing Manager interface during this process. For best results, limit your range of addresses to a maximum of 255.

5. The **Start managing once discovered** check box is selected by default. This enables Avaya Video Conferencing Manager to attempt to log into a device after discovering it, maintain communication with the device, and enables you to manage the device through Avaya Video Conferencing Manager. Consider clearing this check box if you have fewer licenses in Avaya Video Conferencing Manager than devices on your network or you do not wish to manage certain devices in Avaya Video Conferencing Manager.
6. Click the **Start Discovery** button.

## Discovering Devices Registered to a Gatekeeper

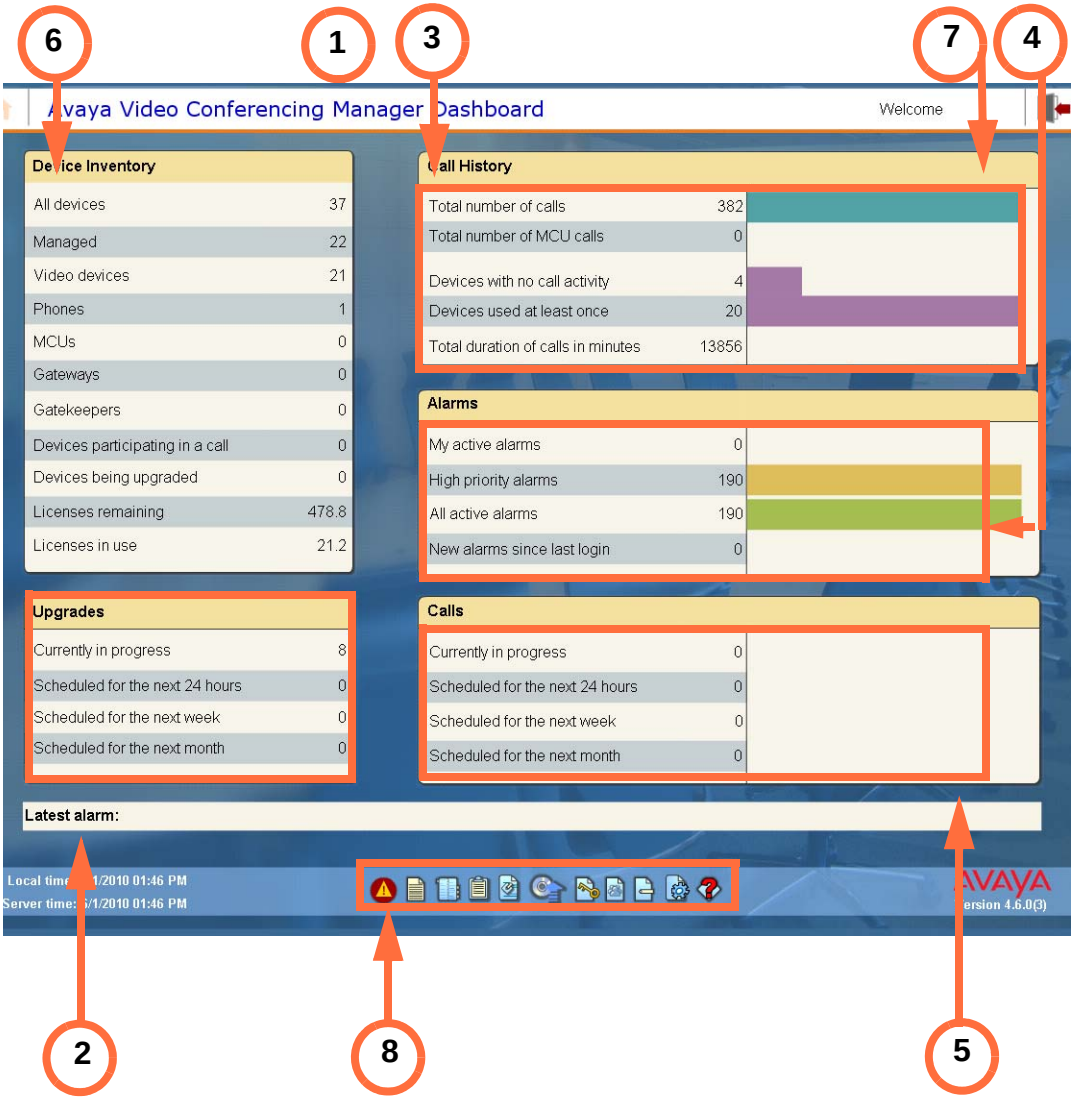
Avaya Video Conferencing Manager automatically discovers gatekeepers, but not the devices registered to them. If a gatekeeper appears on the **Devices** page after you discover devices, complete the following steps to discover the devices registered to the gatekeeper:

1. On the **Devices** page, locate each entry for a discovered gatekeeper.
2. Right-click the entry and click **Discover registered devices**.

   The status of the discovery appears at the bottom of the page and the device list refreshes automatically.

## Using the Avaya Video Conferencing Manager Dashboard

The Avaya Video Conferencing Manager Dashboard provides a comprehensive view of your video and voice communications systems and their status, at a glance.



1. **Device Inventory**—lists the number of known devices and the total number of licenses purchased and in use
2. **Upgrades**—lists scheduled and in-progress device upgrades
3. **Call History**—lists call history and statistics at a glance
4. **Alarms**—lists current alarms and alarm history
5. **Calls**—lists current and scheduled calls

Click any row in these sections of the dashboard to obtain more detailed information or perform a variety of management tasks.

6. Home icon—Click this icon to return to the Avaya Video Conferencing Manager Dashboard from any screen.
7. Log off icon—Click this icon to log off from Avaya Video Conferencing Manager.
8. A row of icons forms a navigation bar at the bottom of the screen and provides access to the following features and functionality.

   ***Note:*** Only those icons associated with features to which the logged in user has access appear in the navigation bar. For more information about user accounts, refer to “Managing User Accounts” on page 40.

| Icon | Mouse-over Text | Description |
|---|---|---|
| | **Alarms** | View and manage alarms. |
| | **Devices** | Discover and manage devices in the network. |
| | **Events** | View, manage, and schedule calls, template actions, device offline schedules and upgrades. |
| | **Reports** | Generate a variety of periodic reports, inventories, summaries, and diagnostics. |
| | **Templates** | Create templates for devices, and backup and restore devices.<br>Available to administrators only. |

| Icon | Mouse-over Text | Description |
|---|---|---|
| | **Packages** | Upload upgrade packages to Avaya Video Conferencing Manager.<br>Available to administrators and engineers only. |
| | **Password** | Specify default passwords for devices and protocols.<br>Available to administrators only. |
| | **User Management** | Add or import, delete, or modify Active Directory or OpenLDAP users. |
| | **License Manager** | Activate Avaya Video Conferencing Manager software.<br>Available to administrators only. |
| | **Avaya Video Conferencing Manager Administrator** | Launches Avaya Video Conferencing Manager Administrator.<br>Available to administrators only. |
| | **Help** | Access user help. |

## Configuring Microsoft Exchange Server

If you enabled integration with Microsoft Exchange Server when you installed Avaya Video Conferencing Manager, you can add Microsoft Exchange Server mailbox resources for your managed video and voice communications systems and MCUs. Once you create the mailbox resources in Microsoft Exchange and register your managed communications systems with those mailboxes, Microsoft Outlook users can schedule those devices as required participants or locations in meeting requests. Those scheduled meetings then appear as scheduled calls within Avaya Video Conferencing Manager on the **Events** page. Calls scheduled through Avaya Video Conferencing Manager also appear as meetings in Microsoft Outlook, thus preventing double booking.

When you schedule an upgrade, a template comparison, or take a communications system offline in Avaya Video Conferencing Manager, that information is shared with Microsoft Outlook and the device becomes unavailable for scheduling other events.

You can change the Microsoft Exchange configuration details and authentication credentials you entered during installation using Avaya Video Conferencing Manager Administrator. For information about Avaya Video Conferencing Manager Administrator, refer to “Using Avaya Video Conferencing Manager Administrator” on page 88.

### Microsoft Exchange Server 2003

The following instructions for creating mailbox resources and registering them with Avaya Video Conferencing Manager apply specifically to Microsoft Exchange Server 2003. If you are using Microsoft Exchange Server 2007, refer to “Microsoft Exchange Server 2007” on page 38.

Complete the following steps to create the mailbox resources needed to integrate Microsoft Outlook scheduling with Avaya Video Conferencing Manager.

***Note:*** If you intend to associate a managed video or voice communications device with the email address of a mailbox for the conference room in which the device resides (deployment option 1 in “Microsoft Exchange Server Integration Overview” on page 9) and you already have room mailboxes in Microsoft Exchange for scheduling purposes, begin with step 7. If you intend to allow meeting participants to add an MCU to a meeting scheduled through Microsoft Outlook, begin with step 1 to create a mailbox resource for each MCU.

1. Navigate to **Programs->Microsoft Exchange->Active Directory Users and Computers**.
2. Create a new user. Right-click the directory icon containing the Active Directory users and select **New Object - User**.

3. Enter the **Full name**, and **User logon name** and click **Next**.
4. Enter and confirm the user's password, select **Password never expires** and click **Next**.
5. Select **Create an Exchange mailbox** and enter an **Alias**, **Server**, and **Mailbox Store**. Click **Next**.
6. Click **Finish**.
7. Configure forwarding of the messages sent to this mailbox to include Avaya Video Conferencing Manager's listener mailbox.
    a. Right-click the user you created in step 5 and select **Properties**. Click the **Exchange General** tab of the **Properties** dialog box. Enter the **Mailbox store**. Click **Delivery Options**.
    b. Select **Forward to** from the **Forwarding address** section of the **Delivery Options** dialog box and click **Modify**. In the **Enter the object name to select** box, enter the mailbox you created for Avaya Video Conferencing Manager during installation and select **OK**.
    c. Select **Deliver message to both forwarding address and mailbox** and click **OK**.
8. If you are configuring a mailbox for an MCU, skip to the next step. For all other mailboxes, register the mailbox for Auto Accept Agent to automatically process meeting requests. For more information, refer to the Registering Mailboxes section of the Microsoft TechNet website: http://technet.microsoft.com/en-us/library/bb124104(EXCHG.65).aspx
9. Ensure that the Microsoft Outlook email box has the correct setting for current time zone. (Refer to Microsoft Outlook help to access this option.) This is crucial for proper scheduling.
10. Register the mailbox you created for the conference room (deployment option 1) or the device (deployment option 2 and MCU mailboxes) with the corresponding voice or video communications system in Avaya Video Conferencing Manager. Refer to "Registering Mailboxes with Devices in Avaya Video Conferencing Manager" on page 39.

    ***Note:*** It may take up to five minutes for the new user to be active and available after you create it.

### Microsoft Exchange Server 2007

The following instructions apply specifically to Microsoft Exchange Server 2007. If you are using Microsoft Exchange Server 2003, refer to “Microsoft Exchange Server 2003” on page 36.

***Note:*** If you intend to associate a managed video or voice communications device with the email address of a mailbox for the conference room in which the device resides (deployment option 1 in “Microsoft Exchange Server Integration Overview” on page 9) and you already have room mailboxes in Microsoft Exchange for scheduling purposes, begin with step 6. If you intend to allow meeting participants to add an MCU to a meeting scheduled through Microsoft Outlook, begin with step 1 to create a mailbox resource for each MCU.

Complete the following steps to create the mailbox resources needed to integrate Microsoft Outlook scheduling with Avaya Video Conferencing Manager.

1. Start the Microsoft Exchange Management Console.
2. Create a mailbox for the conference room that houses your video communications system. Under **Recipient Configuration**, right-click the **Mailbox** icon and select **New Mailbox**.
3. Select **Room Mailbox** for mailbox type and click **Next**.

   ***Note:*** Select **Room Mailbox** even if you are creating a mailbox for a device, including an MCU, as described in Option 2 in “Microsoft Exchange Server Integration Overview” on page 9.
4. Create a new user or select a current user if the conference room in which you have your audio and video communications system already has a user in Active Directory.
5. Enter an alias for the user and select the appropriate Mailbox database. Click **Next**. The mailbox and the corresponding user are created.
6. To set up forwarding to Avaya Video Conferencing Manager’s listener mailbox, double-click the mailbox created in step 5 and select the **Mail Flow Settings** tab. Double-click **Delivery Options**.
7. Select the check boxes for **Forward To** and **Deliver message to both forwarding address and mailbox** and click the **Browse** button. Select the mailbox you created for Avaya Video Conferencing Manager during installation and select **Finish**.
8. To enable the user so that you can associate it with a video communications system, start the Active Directory User Management Console.
9. Locate the user you created in step 5. Right-click and select **Enable**.

10. Right-click and select **Reset Password**.
11. Enter and confirm the password and select **Password never expires**.
12. If you are creating a mailbox for an MCU, skip to step 16.
13. In Microsoft Outlook Web Access, log on to the email account for the video communications system and click **Options** in the upper right-hand corner of the window.
14. In the **Options** menu click **Resource Settings** and enable **Automatically process meeting requests and cancellations**.
15. Click the **Save** button.
16. Ensure that the Microsoft Outlook email box has the correct setting for current time zone. (Refer to Microsoft Outlook help to access this option.) This is crucial for proper scheduling.
17. Register the mailbox you created for the conference room (deployment option 1) or the device (deployment option 2 and MCU mailboxes) with the corresponding voice and video communications system in Avaya Video Conferencing Manager. Refer to “Registering Mailboxes with Devices in Avaya Video Conferencing Manager” on page 39.

    ***Note:*** It may take up to five minutes for the new user to be active and available after you create it.

**Registering Mailboxes with Devices in Avaya Video Conferencing Manager**

1. In Avaya Video Conferencing Manager, click the **Devices** icon in the navigation bar.
2. On the **Display** list, select **Managed: all**.
3. Locate the device you wish to associate with the mailbox resource that you created in Microsoft Exchange.
4. Click the yellow envelope icon in the far right column. The **Register with mailbox** dialog box appears.

5. Enter the mailbox resource you created for it and click **Register**. Avaya Video Conferencing Manager confirms successful registration both by changing the yellow envelope icon from to and by writing a confirmation message to the **Status** box below the list of devices.

   ***Note:*** If the mailbox registration fails, Avaya Video Conferencing Manager writes an error message to the **Status** box below the list of devices. Some of the possible reasons for failure include:

   - Mail forwarding from the device mailbox to the Avaya Video Conferencing Manager mailbox you set up during installation is not in effect. Ensure the mailbox resource for the device in Microsoft Exchange Server is set up to forward its messages to the Avaya Video Conferencing Manager mailbox.
   - Avaya Video Conferencing Manager cannot contact the Microsoft Exchange Server.
   - The Microsoft Exchange Server authentication credentials (domain name, username and password of the Avaya Video Conferencing Manager mailbox, and whether HTTPS access is required) entered during the installation of Avaya Video Conferencing Manager are incorrect.
   - The mailbox is already registered to another managed device.

   ***Note:*** You can unregister the mailbox address from the **Register with mailbox** dialog box by clicking **Unregister**.

## Managing User Accounts

Avaya Video Conferencing Manager supports multiple users and controls user access to functionality through the use of roles. Each user account is associated with one of the following roles:

- **Administrator**

  Administrators have full access to all functionality.

- **Engineer**

  Engineers can perform many of the same tasks as an administrator, except export or assign alarms; manage or modify device settings; create or apply templates; take devices offline; add or delete users; back up and restore a device; and access Avaya Video Conferencing Manager Administrator.

- **Operator**

  Operators can view alarms, device settings, and a list of users; and schedule and manage calls.

For more information about access to specific functionality for each user role, refer to “Appendix A: User Role Access” on page 101.

***Note:*** New users are automatically assigned the Operator role. Refer to “Adding a User Account” on page 41 for details about adding a user. Refer to “Modifying a User Account” on page 42 for details about changing a user’s role.

If you are using the Microsoft Exchange Server integration feature with Avaya Video Conferencing Manager, be aware that Microsoft Outlook users can affect scheduling of calls and adding external devices to Avaya Video Conferencing Manager without having an Avaya Video Conferencing Manager user account. For more information, refer to “Preparing for an Avaya Video Conferencing Manager Deployment” on page 5.

## Adding a User Account

To manage user accounts, click the **User Management** icon on the navigation bar. A list of defined registered users for Avaya Video Conferencing Manager appears.

Avaya Video Conferencing Manager categorizes defined users for Windows-based authentication. Depending on the type of user authentication you chose when installing Avaya Video Conferencing Manager, different options for user management appear.

***Note:*** New users are automatically assigned the Operator role. Refer to “Modifying a User Account” on page 42 for details about changing roles.

### Importing Users from Active Directory

If you chose Active Directory for user authentication when you installed Avaya Video Conferencing Manager, you can import Active Directory users by completing the following steps:

1. On the **Actions** list, choose **Import Active Directory users** and click **Submit**.

   The **Import Active Directory users** dialog box appears and lists the first 100 users.

2. You can import selected users in the list by clicking the names of the users you want to import. Use the **Search** box to search for a specific user name and click **Submit**. You can also change any user account information (such as name, category, location, email, or contact number) by clicking **Next** after selecting the user and before completing the import.

3. Click **Import Selected** to import selected users or click **Import all** to import all users that appear in the dialog box.

***Note:*** If you are using Active Directory for user authentication, you must change user passwords outside of Avaya Video Conferencing Manager.

### Adding Users from OpenLDAP

If you chose OpenLDAP for user authentication when you installed Avaya Video Conferencing Manager, you can add new users as follows:

1. Click the **User Management** icon on the navigation bar.
2. Click the **Add User** button.
3. Enter a login name for the user.
4. Enter a user name for the user.
5. Enter an email address for the user.
6. Click the **Update** button and enter a password for the new user.

   ***Note:*** Passwords for OpenLDAP users are case sensitive.
7. Click **Submit**.
8. Click the **Save** button to add the user.

## Modifying a User Account

To modify an existing user account, follow these steps:

1. Click the **User Management** icon on the navigation bar.

   The **User Management page** appears.
2. Double-click the entry for the user whose account you wish to modify, or right-click the entry and then click **Modify User**.
3. Update the fields you wish to change. You can assign a different role to the user in this step. Refer to “Managing User Accounts” on page 40 for more information about roles.
4. Click the **Save** button to save your changes.

## Deleting a User Account

To delete an existing user account, follow these steps:

1. Click the **User Management** icon on the navigation bar.
2. Right-click the user you wish to delete and click **Delete User**.
3. Click **Yes** to confirm the deletion.

   The user account is removed from the user list.

## Managing Devices

After you discover and enable Avaya Video Conferencing Manager to manage devices, you can perform a variety of management tasks on these devices from the **Devices** page. For information about discovering devices, refer to “Discovering Devices” on page 31. To access the **Devices** page, click the **Devices** icon on the navigation bar or click any device category in **Device Inventory** on the **Avaya Video Conferencing Manager Dashboard**.

Devices appear on the **Devices** page with the following information:

- **Status**: Displays the status of the managed device. Refer to “Status Icons” on page 45 for a description of these icons. Additional status information appears at the bottom of the page when you perform an action on the page. Mouse over an icon to view text that describes the icon.

  ***Note:*** If you did not allow Avaya Video Conferencing Manager to attempt to manage devices during the initial discovery, all discovered devices appear with the **Discovered** status icon on the **Devices** page. To enable Avaya Video Conferencing Manager to manage these devices, right-click the device entry on the **Devices** page and then click **Start managing**.
- **Make**: Indicates the device brand name (for example, Avaya, LifeSize, Polycom, or Tandberg).
- **Model**: Defines the device model name (for example, Avaya 1040).
- **Device Type**: Shows a pictorial representation of the device type. If the type is unknown, a question mark inside a circle appears in this column.
- **IP Address**: Identifies the IP address of the managed device.
- **System Name**: Identifies the name of the device.

  ***Note:*** You can edit the name of a managed device by clicking this field and entering a new name. You can enter only the following characters in this field:

  A-Z a-z 0-9 ~ ! @ # $ % ^ & * ( ) _ - + = { } | \ < , > . ? / ; : \
- **Software Version**: Defines the version of software installed on the managed device.

- Depending on the device type and its status, one or more of the following icons may appear in the far-right column. Text that describes an icon's meaning appears when you mouse over the icon.

| Icon | Description |
|---|---|
| | This icon appears only if you opted to enable Microsoft Exchange Server integration when you installed Avaya Video Conferencing Manager and only for managed devices that can be scheduled in a call using the Microsoft Exchange Server integration feature. For more information about using these icons, refer to "Registering Mailboxes with Devices in Avaya Video Conferencing Manager" on page 39. For more information about using features available with Microsoft Exchange Server integration, refer to "Scheduling Conferences in Microsoft Outlook" on page 80. |
| | Indicates whether affinity to an MCU is set on the device. For more information, refer to "Setting or Clearing MCU Affinity" on page 55. |
| | Indicates whether the device has been registered with a gatekeeper. For more information, refer to "Registering a Device to a Gatekeeper" on page 56. |
| | View the device's calendar. Refer to "Scheduling a Conference in Avaya Video Conferencing Manager" on page 75. |
| | Opens a text box for sending a message to the device. The message appears in the display of the device. For more information, refer to "Sending a Message to a Device" on page 57. |

## Status Icons

The following icons represent the device status. Mouse over an icon to view text that describes the icon.

| Icon | Status |
|---|---|
| | Discovered<br>To enable Avaya Video Conferencing Manager to manage this device, right-click the device entry, and then click **Start managing**. |
| | Login failed. Update the password.<br>Refer to “Managing Device Passwords” on page 58 to update the password. |
| | Responding |
| | Unreachable |
| | Rebooting |
| | Managing |
| | Updating device information |
| | Deleting |
| | External device. Refer to “Adding a New External Device” on page 48. |
| | Dialing |
| | Ringing |

| Icon | Status |
|---|---|
| | Call in progress |
| | Two-way inbound call |
| | Two-way outbound call |
| | Multipoint inbound call |
| | Multipoint outbound call |

## Displaying Devices

On the **Display** list, choose the category of devices to view. Display categories include the following:

| Display Category | Description |
|---|---|
| All | All discovered and external devices |
| Managed: all | Devices that are managed by Avaya Video Conferencing Manager. A managed device is a device that Avaya Video Conferencing Manager monitors for activity, status transitions, and any system alerts or failures. |
| Managed: available | Managed devices that are responding to a ping from Avaya Video Conferencing Manager |
| Managed: not available | Managed devices that are not responding to a ping from Avaya Video Conferencing Manager |
| Video devices | All managed video communications devices |
| Phones | All managed phones |

| Display Category | Description |
|---|---|
| MCUs | All managed multipoint control units |
| Gateways | All managed gateways |
| Gatekeepers | All managed gatekeepers |
| Unmanaged | Devices with a **Discovered** or **Login failed** status icon in the Status column |
| Devices in a call | All managed devices that are currently in a call |
| Devices being upgraded | All managed devices currently being upgraded |
| External Devices | All external devices. For more information, refer to “Adding a New External Device” on page 48. |
| Infrastructure devices | All managed MCUs, gateways, and gatekeepers |
| Devices with alarms | All managed devices with active alarms |
| Calls scheduled within 24 hours | Devices that are scheduled to be in a call within the next 24 hours |
| Devices with no call activity | Devices with no call activity since they were first managed by Avaya Video Conferencing Manager |
| Devices used at least once | Devices used at least once since they were first managed by Avaya Video Conferencing Manager |
| Devices without a mail box | For installations integrated with Microsoft Exchange Server, lists devices that do not have an email address registered to the device. For more information, refer to “Registering Mailboxes with Devices in Avaya Video Conferencing Manager” on page 39. |

The number of devices in the category that you select from the **Display** list (*x*) and the total number of devices that are managed; discovered; discovered, but login failed; and external devices (*y*) appear on the **Devices** page heading as **Devices (*x*/*y*)**.

To search for a single device, enter any alphanumeric string in the **Search** field located in the lower right corner of the page. The search field is case sensitive.

## Adding a New External Device

You can add an external device to the **Devices** page to identify devices that are frequently used in calls but may be unreachable by Avaya Video Conferencing Manager, such as a device that you do not wish to manage in Avaya Video Conferencing Manager or a device not on your organization's network. At minimum, you must enter a name and an IP address. The new device then becomes available to the **Schedule Call** page and appears in the list of devices to select for the call when you click **Add Device** to select devices to schedule in a call. The device also appears on the **Devices** page as an external device.

When you right-click an external device entry on the **Devices** page, you can access the **View details** page where you can enter additional information about the device that you wish to know and that may be useful when including the device in a call, such as the device make, model, and location. You can also join an external device to an existing conference call or delete the device from the **Devices** page by right-clicking the device's entry on the **Devices** page and clicking **Join conference**, or **Delete device** respectively.

***Note:*** If Microsoft Exchange Server integration is enabled in your installation, Avaya Video Conferencing Manager can automatically add external devices to the **Devices** page if a human participant in a call scheduled through Microsoft Outlook responds to a confirmation email by specifying an IP address of an external device as the number at which the participant can be reached. For more information about this feature, refer to "Specifying a Preferred Method of Participation" on page 83.

To add a new device to your managed network, follow these steps:

1. Click the **Devices** icon on the navigation bar or click one of the device-related rows in the **Device Inventory** section of the Avaya Video Conferencing Manager Dashboard.
2. Select **Add a new external device** from the **Actions** list.
3. Click **Submit**.
4. Enter the details for the new device. The system name and IP address are required.
5. Click **Save**.

You can view a list of all external devices added to Avaya Video Conferencing Manager by choosing **External devices** on the **Display** menu.

## Refreshing Device Information

You can refresh information that appears on the **Devices** page for all devices or for a single device.

### Refresh Information for all Devices

1. On the **Actions** menu, click **Refresh all.**
2. Click **Submit**.

### Refresh Information for a Single Device

1. Right-click the device entry.
2. Click **Refresh**.

## Accessing Device Management Features

Management tasks that you can perform depend on the device's type and status. Right-click a device entry to view the tasks available for that device. Tasks appear on a menu and may include one or more of the following:

| Task | Device Type | Description |
|---|---|---|
| View details | All managed and external devices | Refer to "Viewing and Editing Device Details" on page 51 for viewing device details of managed devices. Refer to "Adding a New External Device" on page 48 for viewing details of an external device. |
| Launch browser interface | All managed devices | Launches the device's browser interface. Refer to "Accessing a Device's Web User Interface" on page 58. |
| Update password | All managed devices except gatekeepers | Refer to "Managing Device Passwords" on page 58. |
| Change Password | All managed devices except gatekeepers, gateways, LifeSize Networker, LifeSize Multipoint, Radvision MCUs, and Sony PCS-XG80. | Refer to "Managing Device Passwords" on page 58. |

| Task | Device Type | Description |
|---|---|---|
| View Alarms | Managed video and voice communications devices except Sony PCS-XG80 | Opens the Alarms page and shows the alarms for the device. For more information about alarms, refer to “Managing Device Alarms” on page 63. |
| Create Template | Managed Avaya and LifeSize video communications systems only | Create a configuration template from an existing managed Avaya video communications system. For more information, refer to “Using Templates to Configure Devices” on page 66 |
| Refresh | All managed devices | Refreshes the device’s status. For more information, refer to “Refreshing Device Information” on page 49. |
| Join Conference | Video and voice communications systems only | Joins the device to a call in progress. |
| Schedule Call | Managed video or voice communications device and MCUs | You can select multiple devices by Ctrl-clicking or Shift-clicking them. You can then right-click the selected devices and choose **Schedule call**. Avaya Video Conferencing Manager opens the **Schedule call** page and adds the devices to the schedule. For more information about scheduling calls, refer to “Scheduling Calls and Other Device Events” on page 69. |
| Schedule Upgrade | All managed video and voice communications devices except Sony PCS-XG80 | Schedules a software upgrade for the device. An upgrade package must be present to schedule an upgrade. Refer to “Upgrading Devices” on page 65. If you select multiple devices of the same make and model using the CTL or SHIFT keys, and then right-click the selected group and choose this task, Avaya Video Conferencing Manager opens the **Schedule upgrade** page and adds the devices to the upgrade. |

| Task | Device Type | Description |
|---|---|---|
| Reboot | All devices except gatekeepers and Sony PCS-XG80 | Reboots the device. The device must not be in use. You can safely reboot the device when the **Responding** icon appears as the device status. Refer to “Rebooting a Device” on page 59. |
| Delete Device | All devices | Deletes a device entry from the **Devices** page and from all scheduled calls and events. If the device is the host in a scheduled call, the call is deleted. |
| Take device offline | All managed devices except gatekeepers, gateways, and LifeSize Networker | Prevents a device from being scheduled for a call, an upgrade, and, if applicable, a template event during the specified offline time period. Avaya Video Conferencing Manager continues to manage the device but does not allow access to device settings. This may be useful, for example, if you wish to perform extended maintenance on a device or restrict its use over a specified period of time.<br>Refer to “Scheduling Offline Time for a Device” on page 74. |

## Viewing and Editing Device Details

For each managed device, you can access a **Device details** page from which you can do the following:

- View system information, including edit the system name and locale settings.
- Set the default service prefix for a Radvision or LifeSize MCU. Refer to “Setting a Default Service Prefix for an MCU” on page 52.
- Specify northbound settings for forwarding traps for a device. Refer to “Forwarding SNMP Traps with Northbound Settings” on page 53.
- Access the same icons that appear in the far right corner for the device on the **Devices** page and view the device’s status icon. Refer to the descriptions of these icons in “Managing Devices” on page 43.

- If the device is an Avaya video communications system, you can also access many of the configuration preferences that are available in the device's web administration interface and show video snapshots.

***Note:*** For external devices, Avaya Video Conferencing Manager offers a device details page on which you can record information about the device. For more information about external devices, refer to "Adding a New External Device" on page 48.

To access the **Device details** page for a managed device, follow these steps:

1. Click the **Devices** icon on the navigation bar.
2. Right-click the managed device you wish to edit and then click **View details**.

   ***Note:*** You can also access the **Device details** page from the **Schedule Call** page when you schedule a call for the device. Each device added to the **Schedule Call** page appears as a link. Click the link to open the **Device details** page. For more information about using the **Device details** page from the **Schedule Call** page, refer to "Scheduling a Conference in Avaya Video Conferencing Manager" on page 75.
3. Make your changes.

   ***Note:*** You can enter only the following characters in text boxes on the **Device details** page: A-Z a-z 0-9 ~ ! @ # $ % ^ & * ( ) _ - + = { } | \ < , > . ? / ; : \
4. Click **Save**.

## Setting a Default Service Prefix for an MCU

You can set a default service prefix for a managed Radvision or LifeSize MCU from the **Device details** page. A service prefix identifies a service created on the MCU. For information about creating services on the MCU, refer to the product documentation that accompanies the MCU.

1. Access the **Devices** page.
2. On the **Display** list, click **Managed: all**.
3. Right-click the device entry of the MCU and click **View details**. The **Device details** page appears.

   ***Note:*** You can also access the **Device details** page from the **Schedule Call** page when you schedule a call for the device. Each device added to the **Schedule Call** page appears as a link. Click the link to open the **Device details** page. Changing the service prefix on the **Device details** page when scheduling a call, changes the prefix only for that call.

4. On the **System information** tab, locate the **Generic properties** page.
5. In the **Service prefix** list, click the service prefix you wish to use. The maximum bandwidth and maximum participants for that prefix appear below the list.

   ***Note:*** If the service prefix you select is subsequently deleted on the MCU, Avaya Video Conferencing Manager chooses the next available prefix with the highest bandwidth allowed. If no services are registered on the MCU, a scheduled call with this MCU fails.
6. Click **Save**.

## Forwarding SNMP Traps with Northbound Settings

Avaya Video Conferencing Manager supports management of video communications devices through standard APIs including Simple Network Management Protocol (SNMP). SNMP is a standard mechanism for tracking configuration and status of a system. SNMP allows for connection to third-party management frameworks.

Using SNMP version 3, you can send SNMP traps from Avaya Video Conferencing Manager to a management system such as a northbound SNMP receiver. This functionality is useful to networking companies using trap complexes. You can configure one or more SNMP trap hosts and send copies of traps for further use with data mining tools to show trends on the network.

Trap forwarding in Avaya Video Conferencing Manager is available only for managed video and voice communications devices. This feature is not available for managed gatekeepers, gateways, and MCUs.

You can specify external SNMP trap destinations to which Avaya Video Conferencing Manager forwards traps from a single managed device using the **Northbound** tab on the **Device details** page of the device. You can also use the **Northbound Settings** page in Avaya Video Conferencing Manager Administrator to specify global trap destinations to forward all traps from all managed video and voice communications devices or to enable or disable trap forwarding.

If you configure global trap destinations, each global trap destination appears as an entry on the **Northbound** tab on the **Device details** page of each managed video and voice communications device. The global destination icon appears in the **Actions** column to indicate a global trap destination. You cannot edit a global trap destination from the **Device details** page.

By default, trap forwarding is enabled. To disable trap forwarding, clear the **Enable Avaya Video Conferencing Manager Northbound Settings** check box on the **Northbound Settings** page in Avaya Video Conferencing Manager Administrator and refresh your browser. If you disable trap forwarding, the **Northbound** tab on the **Device details** page does not appear. For more information about using Avaya Video Conferencing Manager Administrator, refer to “Using Avaya Video Conferencing Manager Administrator” on page 88.

***Note:*** If you configure global trap destinations in Avaya Video Conferencing Manager Administrator and trap destinations on the **Device details** page for a single device, Avaya Video Conferencing Manager forwards traps for that device to all trap destinations specified in both Avaya Video Conferencing Manager Administrator and on the **Device details** page.

Follow these steps to specify a trap destination to forward traps from a single device:

1. Access the **Devices** page.
2. In the **Display** list, click **Managed: all**.
3. Right-click the managed device from which to forward alarms and then click **View details**. The **Device details** page appears.
4. Click the **Northbound** tab.

   ***Note:*** If trap forwarding is disabled in Avaya Video Conferencing Manager Administrator, the **Northbound** settings on the **Device details** page are not available.
5. Click the **Add** button. The **Add new destination** dialog box appears.
6. Enter the following information about the SNMP trap destination:
   - IP address
   - port number that the remote SNMP manager is listening on for traps
   - username (not to exceed 40 characters)
   - password (not to exceed 40 characters)
7. Click **Save**. The entry appears in the table above the **Add** button.

   ***Note:*** To edit or delete an SNMP trap destination, click the **Modify this entry** icon or **Remove this entry**  icon in the **Actions** column for the entry you wish to modify or delete.

## Setting or Clearing MCU Affinity

You can use cascading MCUs to connect calls between two groups of participants. Each groups' communication is channeled through one MCU, and the MCUs pass the bundled communication between each other, greatly reducing the bandwidth needed for the groups to communicate with each other. To use this optional feature when scheduling a call, the devices in the call must be assigned affinity to an MCU.

Assigning MCU affinity to devices has additional benefits. If you schedule a call in Avaya Video Conferencing Manager and none of the devices has the capacity to host the call, Avaya Video Conferencing Manager prompts you to add an MCU and asks if you would like Avaya Video Conferencing Manager to make the selection for you. If you allow Avaya Video Conferencing Manager to select the MCU, Avaya Video Conferencing Manager makes the selection based first on the MCU affinity of the participating devices, if assigned.

If you enabled and configured Microsoft Exchange Server integration with Avaya Video Conferencing Manager, be aware that cascading MCUs are not available to participants who schedule calls in Avaya Video Conferencing Manager through Microsoft Outlook. However, if a meeting organizer in Microsoft Outlook selects more that one MCU to participate in a call, or fails to select an MCU and one is needed for the call, Avaya Video Conferencing Manager automatically selects one MCU if a managed MCU is available and makes the selection based first on the MCU affinity of the participating devices, if assigned.

To assign MCU affinity to a device, follow these steps:

1. Access the **Devices** page.
2. On the **Display** list, click **Managed: all**.
3. Locate the entry for the device that you wish to associate with an MCU and click the Set MCU affinity icon in the far-right column. The **Set the MCU Affinity** dialog box appears.

   ***Note:*** This icon is also available on the upper-right corner of the **Device details** page. Refer to “Viewing and Editing Device Details” on page 51 for information about accessing the **Device details** page. MCU affinity is not available for external devices.
4. Select an MCU from the **Select the MCU** list.

   ***Note:*** If a managed MCU does not exist in Avaya Video Conferencing Manager, the **Select the MCU** list is not available.
5. Click the **Set the MCU Affinity** button. The MCU affinity icon in the device entry changes to indicate that MCU affinity is set for the device.

   ***Note:*** You can clear the MCU affinity set for a device by clicking the **Clear the MCU Affinity** button in the **Set the MCU Affinity** dialog box.

For more information about using cascading MCUs when scheduling a call, refer to “Using Cascading MCUs” on page 78.

## Registering a Device to a Gatekeeper

You can register a managed device to a managed gatekeeper by completing the following steps:

1. Access the **Devices** page.
2. On the **Display** list, click **Managed: all**.
3. Locate the entry for the device that you wish to register with a gatekeeper and click the register with gatekeeper icon in the far-right column. The **Register with gatekeeper** dialog box appears.

   ***Note:*** This icon is also available on the upper-right corner of the **Device details** page. Refer to “Viewing and Editing Device Details” on page 51 for information about accessing the **Device details** page.
4. By default, the **Gatekeeper** option is selected. On the **Select the gatekeeper** list, select a managed gatekeeper.
5. Click the **Register** button. The register with gatekeeper icon in the device entry changes to indicate that the device is registered to a gatekeeper.

   ***Note:*** You can unregister a device that is registered to a gatekeeper by clicking the **Unregister** button in the **Register with gatekeeper** dialog box.

## Sending a Message to a Device

You can send a message to a managed video communications device to appear in the display connected to the device. The message appears in a dialog box with an **OK** button for users to acknowledge and close the message.

***Note:*** This feature is available only for managed Avaya, LifeSize, Polycom, and Tandberg video communications systems. If not acknowledged, the message closes after 10 seconds on Avaya and LifeSize video communications systems only.

To send a message, follow these steps:

1. Access the **Devices** page.
2. On the **Display** list, click **Managed: all**.
3. Locate the entry for the device to which you wish to send a message and click the **Show message on device** icon in the far-right column.

   ***Note:*** This icon is also available on the upper-right corner of the **Device details** page. Refer to “Viewing and Editing Device Details” on page 51 for information about accessing the **Device details** page.
4. Enter a message in the **Enter the message** text box. Only ASCII characters are allowed. The maximum number of characters allowed depends on the device’s make as follows:
   - Avaya: 200
   - LifeSize: 200
   - Polycom: 100
   - Tandberg: 40
5. Click **Send message**.

## Accessing a Device's Web User Interface

You can open the web user interface of any discovered device to access the configuration options on that device. Refer to the documentation included with your device for more information.

To open a device's web user interface, follow these steps:

1. Access the **Devices** page.
2. Right-click the device that you wish to access.
3. Select **Launch browser interface**.

   ***Note:*** If the device is an Avaya or LifeSize video communications system, Avaya Video Conferencing Manager automatically logs on to the browser interface.

## Managing Device Passwords

When Avaya Video Conferencing Manager attempts to manage a device, it uses the default password that you specify on the **Passwords** page. Refer to "Specifying Default Passwords for Device Management" on page 30. If the device does not use that default password, the device appears on the **Devices** page with an orange key icon in the **Status** column signifying the login failed. You must update the password stored in the Avaya Video Conferencing Manager database for that device before you can manage the device.

***Note:*** The orange key icon also appears after a device is managed if the device's password is changed using a mechanism other than Avaya Video Conferencing Manager (for example, at the command line interface for the device). Refer to "Changing a Device Password" on page 59 to change a managed device's password using Avaya Video Conferencing Manager.

### Updating a Device Password

Updating a password for a device in Avaya Video Conferencing Manager changes the password stored for that device in the Avaya Video Conferencing Manager database. It does not change the password stored on the device. To update the password that Avaya Video Conferencing Manager stores in its database and uses to contact a device, follow these steps:

1. Access the **Devices** page.
2. Right-click the managed device for which you wish to update the password and click **Update Password**.
3. Enter a user name and password.
4. Click **Update**.

### Changing a Device Password

You can use Avaya Video Conferencing Manager to change the password stored on a device only if the device is managed in Avaya Video Conferencing Manager. Changing a password on a managed device changes the password stored on the device and automatically updates the password that Avaya Video Conferencing Manager stores in its database and uses to contact the device.

To change the password on a managed device, follow these steps:

1. Access the **Devices** page.
2. Right-click the managed device for which you wish to change the password and click **Change Password**.

   The **Change Password** dialog box appears.
3. Enter a new password and re-enter it to confirm it.
4. Click **Update**.

## Rebooting a Device

To reboot a managed device, follow these steps:

1. Click the **Devices** icon on the navigation bar or click **Managed** from the **Device Inventory** section of the Avaya Video Conferencing Manager Dashboard.
2. Right-click the managed device you wish to reboot and click **Reboot**.

   ***Note:*** The device must not be in use. You can safely reboot the device when the responding icon appears.
3. Click **Yes**. Avaya Video Conferencing Manager sends a reboot command to the device. The rebooting icon appears.

## Deleting a Device

Deleting a device from Avaya Video Conferencing Manager results in the following actions:

- Avaya Video Conferencing Manager removes the device from the **Devices** page and from all scheduled calls and events in which the device is a participant.
- If the device is a participant in a call scheduled through Microsoft Outlook and Microsoft Exchange Server integration is enabled, Avaya Video Conferencing Manager notifies the meeting organizer of the change.
- If the device is the host in a scheduled call, Avaya Video Conferencing Manager deletes the call.
- Avaya Video Conferencing Manager also deletes any device backups created from the **Templates** page, if applicable.

To remove a device from Avaya Video Conferencing Manager, follow these steps:

1. Click the **Devices** icon on the navigation bar.
2. Right-click the device you wish to delete and then click **Delete Device**. Avaya Video Conferencing Manager removes the device from the **Devices** page.

## Managing a Device Through Email

If you enabled and configured Microsoft Exchange Server integration with your Avaya Video Conferencing Manager installation, Avaya Video Conferencing Manager administrators can send management commands to managed video communications devices using email. The **To** field of the email message must contain the email address of one or more managed devices. Administrators can send an email as plain-text, HTML, or rich-text. The **Subject** field must contain one of the following commands. The commands are not case-sensitive.

| Command | Applies to these Makes | Action Executed on Device |
|---|---|---|
| REBOOT | Avaya<br>LifeSize<br>Polycom<br>Tandberg | Reboots the devices to which the email message is sent. |
| CALL | Avaya<br>LifeSize<br>Polycom<br>Tandberg<br>Sony | Places a conference call that includes the list of devices to which the email is sent. The icon appears in the **Type** column on the **Events** page to identify an adhoc call placed through email using this command.<br>**Note**: This command cannot be used to add devices to a conference call in progress. |
| HELP | Avaya<br>LifeSize<br>Polycom<br>Tandberg<br>Sony | Sends a reply email that lists and describes the commands that can be sent to the device in an email message. A single reply is sent even if the HELP command is sent to multiple devices. |
| HANGUP | Avaya<br>LifeSize<br>Polycom<br>Tandberg<br>Sony<br>Does not apply to MCUs. | Disconnects the list of devices to which the email is sent if these devices are in a call. If any one of the devices is hosting a call, then all participants connected to that host in the call are also dropped. |

| Command | Applies to these Makes | Action Executed on Device |
|---|---|---|
| BACKUP<br>BACK-UP<br>BACK UP | Avaya<br>LifeSize | Backs up the current device settings as a template. |
| CALLSTATS<br>CALL STATS<br>CALL STATISTICS | Avaya<br>LifeSize<br>Polycom<br>Tandberg<br>Sony | Retrieves the calls statistics for all video communications systems to which the email is sent. |
| DESCRIBE<br>DESC | All managed devices | Retrieves the details of the devices to which the command was sent. This information appears on the **Device details** page of a managed device in Avaya Video Conferencing Manager. |
| MESSAGE | Avaya<br>LifeSize<br>Polycom<br>Tandberg | Shows a message in the display of the video communications system. Use only ASCII characters. Non-ASCII characters will not display in the message. Enter the message in the body of the email. Delete signature information or other text that automatically appears in the body of the message.<br>Avaya Video Conferencing Manager truncates messages that exceed the following number of characters:<br>Avaya: 200<br>LifeSize: 200<br>Polycom: 100<br>Tandberg: 40 |
| SNAPSHOT | Avaya<br>LifeSize | Fetches the current video snapshot on the device as a .jpg attachment to a reply email. |

| Command | Applies to these Makes | Action Executed on Device |
|---|---|---|
| AUTOSH | Avaya<br>LifeSize | Executes a command line interface (CLI) command on an Avaya or LifeSize device. Enter AUTOSH in the **Subject** field and the CLI command in the body of the message (for example, `get system name`). |

Avaya Video Conferencing Manager sends an individual response email (success or failure) to indicate the result of the action taken on each of the devices on which a command was executed. If Avaya Video Conferencing Manager does not recognize any of the emails, then no action or response email is sent. Email commands are not supported with external devices.

The **Conference audit report** available from the Reports page includes **EMAIL** as a call source type for calls initiated using email commands. The **User audit report** reflects the conferences initiated by users using email commands. For more information about using reports in Avaya Video Conferencing Manager, refer to “Generating Reports” on page 86.

You can disable this feature by clearing the **Enable device management through email check box** on the **Microsoft Exchange Settings** page in Avaya Video Conferencing Manager Administrator.

For more information about using Avaya Video Conferencing Manager Administrator, refer to “Using Avaya Video Conferencing Manager Administrator” on page 88.

## Managing Device Alarms

The **Alarms** section of the Avaya Video Conferencing Manager Dashboard presents a digest of current alarms. Monitor current alarms by clicking **All active alarms** from the **Alarms** section of the Avaya Video Conferencing Manager Dashboard. Click any alarm entry for more detailed information about that category of alarm.

> ***Note:*** You can disable or enable specific alarms from the **Alarms Configuration** page in Avaya Video Conferencing Manager Administrator. For more information, refer to “Alarms Configuration” on page 89. For a list of alarms by category, refer to “Appendix B: Alarms by Category” on page 106.

You can view alarms for a particular device by clicking **Devices** from the navigation bar, right-clicking the device, and choosing **View alarms**.

Click the **Alarms** icon in the navigation bar to open the **Active Alarms** tab on the **Alarms** page and view active alarms reported for managed devices. Click the **History Alarms** tab to view past alarm events.

Alarms are color-coded to assist you in identifying alarms by severity.

| Color | Severity |
|---|---|
| Red | High |
| Orange | Medium |
| Green | Low |
| Purple | Information |

You can sort alarms by clicking any column heading on the **Active alarms** or **History alarms** tabs. On the **Active alarms** tab, use the **Filter by** list to view a list of alarms by severity, alarms assigned to you, or new alarms since the last time you logged in to Avaya Video Conferencing Manager. On the **History alarms** tab, use the **Filter by** list to view alarms by severity. Use the **Search by** fields at the bottom of the page to refine your search.

On the **Alarms** page, you can manage a single alarm (or multiple alarms by SHIFT-clicking or CTRL-clicking to select them) in a number of ways:

- Acknowledge an alarm by selecting the alarm and choosing **Acknowledge alarm** from the **Actions** list, or right-clicking the alarm and selecting **Acknowledge alarm**. The alarm becomes inactive and moves to the **History alarms** list. You can also right-click an alarm and choose **Acknowledge alarm with resolution** and enter information (up to 500 characters) about how the issue was resolved. On the **History alarms** tab, you can right-click an alarm and choose **Unacknowledge alarm** to move the alarm back to the **Active alarms** page.

  ***Note:*** Users must be authenticated to acknowledge alarms, even if they are not logged in to Avaya Video Conferencing Manager when doing so (for example, when acknowledging an alarm from the email notification).

- Assign an owner to an alarm by choosing **Assign alarm** from the **Actions** list or right-clicking and selecting **Assign alarm**, and then choosing the person to which to assign the alarm from the corresponding list. To assign yourself as the person responsible for resolving the alarm, select the alarm and choose **Own Alarm** from the **Actions** list, or right-click the alarm and select **Own Alarm**. Your name displays in the **Owner** field for that alarm. That alarm then appears in the **My active alarms** list.
- Send alarm information to another user by selecting the alarm and choosing **Forward alarm** from the **Actions** list or right-clicking the alarm and selecting **Forward alarm**. Enter the email address of the recipient and click the **Forward alarm** button.

- Export alarms on the **History alarms** tab. Use the **Export/Backup** list to export all or selected history alarms as a CSV or XML file. You can also access these export options by right-clicking an alarm on the **History alarms** tab.

## Upgrading Devices

Upgrading a device from Avaya Video Conferencing Manager includes the following tasks:

1. Download the upgrade package from the device manufacturer to a location on your network that is accessible to Avaya Video Conferencing Manager.
2. Upload the package to Avaya Video Conferencing Manager.
3. Schedule the upgrade in Avaya Video Conferencing Manager.

### Managing Upgrade Packages

To upload new software packages for your devices, follow these steps:

1. Ensure that you have downloaded an upgrade package from the device manufacturer for the devices you wish to upgrade and that the package resides at a location on your network that is accessible to Avaya Video Conferencing Manager.
2. Click the **Packages** button on the navigation bar.
3. On the **Actions** menu, choose **Upload packages** and click **Submit**.
4. Specify the make, model, and version of the package.
5. Enter the location of the software package or click **Browse** to navigate to it.
6. Click the **Upload** button to upload the package.

   An entry for the package appears on the **Packages** page. You can apply the software upgrade package immediately or schedule it for a later time. Refer to “Scheduling a Device Software Upgrade” on page 73.

   ***Note:*** To remove a package from the list, right-click the package you wish to delete and click **Delete Package**.

## Using Templates to Configure Devices

Templates in Avaya Video Conferencing Manager are stored configurations for Avaya or LifeSize video communications systems that you can apply to a single device or multiple devices simultaneously. Use templates when you want to ensure that these managed devices are consistently configured across your organization to achieve any of the following goals:

- Quickly configure new video communications systems that are added to your network.
- Facilitate use and, consequently, a higher return on investment in these devices by ensuring that users have a uniform experience with video communications systems across the organization.
- Improve troubleshooting and support capabilities for these devices by help desk and information technology personnel. You can compare a device's configuration with a template to determine any discrepancies for troubleshooting purposes, apply a template to resolve a problem associated with a changed configuration, or ensure that systems are set to the company defaults.
- Back up and restore the configuration of a device.
- Deliver a secure environment. You can periodically apply templates with settings that facilitate adherence to security policies in your organization. For example, you can create a template that prevents unauthorized video access to conference rooms when the systems are unattended by disabling automatic call answering; apply encryption in calls; disable control of cameras by far end users; and disable automatically starting a presentation when a presentation device is connected to a system.

You can create a new template and specify the settings manually, or create a template based on an existing device. For a new template, you can specify template parameters based on the device's make, software version, and model or specify a template that contains only common parameters for all models or all models of a selected make.

The following restrictions apply to templates in this release:

- Not all configuration preferences that are available in the device user interface are available in templates.
- You can enter only the following characters in text boxes when creating or editing templates: A-Z a-z 0-9 ~ ! @ # $ % ^ & * ( ) _ - + = { } | \ < , > . ? / ; : \

### Creating and Editing Templates

To create a template, follow these steps:

1. Click **Templates** in the navigation bar.
2. On the **Actions** menu, choose either **Create template** to create a new template **or Create template from device** to create a template based on the configuration of an existing device.
3. Click **Submit**.
4. Depending on the type of template you want to create, do one of the following:
   - If you are creating a new template, enter the details for the template (name, make, version, and model for the device).
   - If you are creating a template from an existing device, select the device from which to create the template and enter a name for the new template.

     ***Note:*** You can also create a template from an existing device from the **Devices** page by right-clicking the device and choosing **Create template**.
5. Click **Ok**.
6. Select the preferences you wish to set and choose the desired preference setting.
7. Click **Save**. An entry for the template appears on the **Templates** page.

   ***Note:*** You can edit a template by double-clicking its entry on the **Templates** page or right-clicking its entry on the **Templates** page and choosing **Edit template**.

### Applying a Template

You can apply a template immediately to one or more devices, or schedule a template application for a future date and time. For more information about scheduling template events, refer to “Scheduling Template Applications and Comparisons” on page 71. To apply a template immediately, complete the following steps:

1. On the **Templates** page, right-click the template you wish to apply and click **Apply template**.

   The **Apply template** dialog box appears.
2. In the **Select devices** list, click the devices to which you wish to apply the template. You can use the SHIFT and CTRL keys to select multiple devices.
3. Click **Ok**. When the **Templates** dialog box appears, click **Ok**.

4. Check for template application errors. On the **Actions** list, select **View logs** and click **Submit**.

   The **View logs** dialog box appears and indicates the status of the operation. The **Failed parameters** list identifies parameters that were not updated correctly during the template application.

### Comparing a Template

You can compare a template immediately to an existing device's configuration, or schedule a template comparison for a future date and time. For more information about scheduling template events, refer to "Scheduling Template Applications and Comparisons" on page 71. To compare a template to an existing device's configuration immediately, complete the following steps:

1. On the **Templates** page, right-click the template you wish to apply and click **Compare template**.

   The **Compare template with device settings** dialog box appears.

2. On the **Select device** list, select the device for which you wish to compare its configuration to the template settings.

3. Click **Ok**.

   The **Compare template with device settings** dialog box appears and lists any differences between the template settings and the current settings on the device.

## Backing up a Device

You can back up and restore configuration settings for individual Avaya and LifeSize video communications systems only. A backup can only be restored on the device from which it was generated. Backup and restore operations are an extension of the templates feature. For more information about templates, refer to "Using Templates to Configure Devices" on page 66. You can perform incremental backups over time and restore them at a later time from the **Templates** page. A backup can only be restored on the device from which it was generated.

To back up a device, follow these steps:

1. Click the **Templates** icon in the navigation bar.

2. Choose **Backup device** from the **Actions** menu.

3. Click **Submit**. The **Backup Device** dialog box appears.

4. Choose the device you want to backup.

5. Enter a description for the backup.

6. Click **Ok**.
7. Name the backup file and save it.

## Restoring a Device from a Backup

To restore settings from a backup file to a device, follow these steps:

1. Click the **Templates** icon in the navigation bar.
2. Choose **Restore device** on the **Actions** menu.
3. Click **Submit**. The **Restore device** dialog box appears.
4. Choose the device to restore.
5. Choose a backup from those available.

   ***Note:*** A backup can only be restored on the device from which it was generated.

6. Click **Ok**.

## Scheduling Calls and Other Device Events

On the **Events** page, you can schedule and view scheduled calls, upgrades, template events, calls or upgrades in progress, devices taken offline, and events for a particular time frame. Click the **Events** icon in the navigation bar and choose an option from the **Display** list.

You can also do the following:

- Sort a list by clicking a heading. For example, to sort events by status, click the **Status** heading.
- Restart terminated and completed calls by right-clicking them and selecting **Dial this call again**, and then clicking **Call Now**.
- View a system calendar of scheduled events by selecting **View System Calendar** from the **Actions** list and clicking **Submit**.

***Note:*** You can also schedule a call, an upgrade, or take a device offline by clicking **Devices** from the navigation bar, right-clicking the desired device, and choosing **Schedule Call**, **Schedule Upgrade**, or **Take device offline**.

If you enabled and configured Microsoft Exchange Server integration with your Avaya Video Conferencing Manager installation, Microsoft Outlook users can schedule video or voice calls using a Microsoft Outlook meeting request. For information about scheduling calls in Avaya Video Conferencing Manager from Microsoft Outlook, refer to “Scheduling Conferences in Microsoft Outlook” on page 80. Calls scheduled from Microsoft Outlook appear on the **Events** page with the icon in the **Type** column.

The following **Status** icons appear on the **Events** page to indicate the status of scheduled events:

| Icon | Description |
|---|---|
| | Call clearing |
| | Call completed |
| | Call in progress |

| Icon | Description |
|---|---|
| | Call pending |
| | Call terminated |
| | Call failed |
| | Updating event information |
| | Template comparison pending |
| | Template comparison in progress |
| | Template comparison successful |
| | Upgrade in progress |
| | Upgrade failed |
| | Upgrade pending |
| | Upgrade successful |
| | Device offline scheduled |

| Icon | Description |
|---|---|
| | Device offline terminated |
| | Device offline completed |
| | Device offline in progress |
| | Device offline failed |

The following event icons can appear in the **Type** column to indicate additional details about an event:

| Icon | Description |
|---|---|
| | A recurring event |
| | A call scheduled from Microsoft Exchange Server. |
| | An adhoc call initiated by an Avaya Video Conferencing Manager administrator using the email-based CALL command. For more information, refer to “Managing a Device Through Email” on page 61. |

## Scheduling Template Applications and Comparisons

You can schedule the application of a template to a device, and make the template application recurrent. Alternatively you can schedule comparisons of templates to the settings of a managed device or devices. Avaya Video Conferencing Manager generates a report of the differences between the template and the settings on the devices and sends it to the email address or addresses you have set up as alert destinations either during installation or in the Avaya Video Conferencing Manager Administrator **Email Settings** page. You can also make these comparisons recurrent.

To schedule template actions, follow these steps:

1. Click the **Events** icon on the navigation bar.
2. On the **Actions** list, choose **Schedule Template**.
3. Click **Submit**.
4. Enter the details for the template action.
   a. Enter a name for the action.
   b. Enter a start date and time and an end date and time.
   c. Select the **Make**, **Model** and **Version**. If you select **common** for **Model**, the action only affects the settings that the devices share with the template.
   d. Select the devices to which you want to apply or compare to the template.
   e. In the **Template name** list, select the template.
   f. In the **Job Type** list, select **Compare** or **Apply**.
   g. Click the **Recurrence** button to set up a regularly occurring template action.

   ***Note:*** In an OpenLDAP installation, you cannot schedule templates beyond six months.

   h. Click **Schedule**.

      The event appears on the **Events** page.

### Checking for Template Application Errors

Errors during the application of a template do not abort the process but are instead collected and noted in the log. To check for errors during a template application follow these steps.

1. Click the **Templates** icon on the navigation bar.
2. On the **Actions** list, select **View logs** and click **Submit**.

   The **Failed parameters** list identifies parameters that were not updated correctly during the template application.

## Scheduling a Device Software Upgrade

To schedule the application of one or more software upgrade packages to your devices, follow these steps:

1. Click the **Events** button in the navigation bar.
2. Choose **Schedule Upgrade** from the **Actions** menu.

   ***Note:*** On the **Devices** page, you can also right-click a managed device, or select multiple devices of the same make and model, and then right-click to schedule an upgrade.
3. Enter a name for the upgrade, the start and end time for the upgrade, and identify the device or devices you want to upgrade.

   ***Note:*** In an OpenLDAP installation, you cannot schedule upgrades beyond six months.
4. Choose a **Make** and **Model** of the device you want to upgrade. For Avaya and LifeSize devices, if you choose **all-endpoints** for the model, all managed video and voice communications devices for the selected make appear in the **Select devices** list. This feature enables you to upgrade multiple models that use the same upgrade package.
5. Select the individual devices from the list.
6. Choose the package you want to apply from the **Packages** list.
7. If you are upgrading a Tandberg device that requires a registration key, enter the key in the **Register Key** text box.

   ***Note:*** Support for upgrades to Polycom devices that require a registration or license key is not available in this release.
8. Click the **Schedule** button to schedule the upgrade or click **Apply Now** to start the upgrade immediately. If you choose **Schedule**, the event appears on the **Events** page as a scheduled event.

   ***Note:*** To delete a scheduled upgrade, select **Scheduled upgrades** on the **Display** menu; right-click the event, and then click **Delete**.

### Viewing Upgrade Schedules

You can also view upgrade schedules by clicking the **Events** icon on the navigation bar and choosing **Scheduled Upgrades** from the **Display** menu.

## Scheduling Offline Time for a Device

You can take a managed device (excluding gatekeepers and gateways) offline for a specified period of time so that Avaya Video Conferencing Manager users (and Microsoft Outlook users if Microsoft Exchange Server integration is enabled) cannot use the device in any scheduled events or manage the device in Avaya Video Conferencing Manager during that time period. This may be useful, for example, when you need to perform maintenance on a device for an extended period of time or isolate a device for dedicated use by a particular group of users.

***Caution:*** If the device is scheduled to participate in another event during the offline time period, Avaya Video Conferencing Manager deletes the scheduled event (if the event depends on the device) or modifies the scheduled event by deleting the device from the event. If the event is a scheduled call in which the device is the host of a cascaded subconference or the only participant in a subconference, Avaya Video Conferencing Manager removes the entire subconference from the call. If the call was scheduled through Microsoft Outlook, Avaya Video Conferencing Manager sends the meeting organizer an email indicating that the device has been removed from the call.

To take a managed device offline, follow these steps:

1. Click the **Events** icon in the navigation bar.
2. On the **Actions** menu, click **Schedule device offline** and click **Submit**.

   The **Schedule Offline for device** dialog box appears.

   ***Note:*** You can also access this dialog box from the **Devices** page by right-clicking a managed device and clicking **Take device offline**.
3. Enter the following information for the event:
   a. Name the event. This name identifies the event when it is listed on the **Events** page.
   b. Ensure that the **Selected device** list shows the IP address and name of the device that you wish to take offline.
   c. Select the date and time period to take the device offline.
   d. Click **Schedule**.
   e. If the device is already a participant in another scheduled event for that time period, Avaya Video Conferencing Manager prompts you to review the list of conflicting events. Click **Yes** to review the list. The **Events** page appears and lists the conflicting events. To clear the conflicts, you can modify the events by right-clicking an event entry and then clicking **Edit Details**.

f. When you are finished viewing or modifying the conflicting events, click **Confirm** at the bottom of the **Events** page to delete or modify the conflicting events and create the offline event. The device offline event appears on the **Events** page as a scheduled event.

## Scheduling a Conference in Avaya Video Conferencing Manager

To schedule conferences from Avaya Video Conferencing Manager, follow these steps:

1. Click the **Events** icon on the navigation bar.
2. Choose **Schedule Call** from the **Actions** list.
3. Click **Submit**. The **Schedule Call** dialog box appears.
4. Enter the details for the call:
   a. Enter a name for the conference so you can identify it in a list of events on the **Events** page.
   b. Choose the reservation type. Choose **Auto Launch** to automatically start the call at the scheduled time, or choose **Reservation Only** to reserve devices for the call, but require manual call placement. When reserved, you cannot schedule devices for maintenance or other purposes.
   c. Select the start and end date and time.
   d. Select the **Auto disconnect** check box to end the call automatically when its scheduled time ends.
   e. Select the **Alert before termination** check box to alert participants of the end of the call 5 minutes before the call is ended.
5. Add participants to the call:
   a. Click **Add Device** to display a list of managed devices.
   b. Add a displayed device by clicking it and clicking the **Add** button or by double-clicking the device. You can select multiple devices by Ctrl-clicking or Shift-clicking additional devices. If you add more than two devices, Avaya Video Conferencing Manager automatically selects the first multipoint-capable device added as the host. If you add more devices to the call than the device currently hosting the call can handle, Avaya Video Conferencing Manager automatically reconfigures the call with a more capable host. You can also change hosts by dragging and dropping a participating device on the device currently selected as the host.

c. If you need to add an external device that is not available for selection in the **Add Device** dialog box, click **Add External Device.** In the **Add External Device** dialog box that appears, specify the protocol to use to connect to the device, enter the IP address or number to use to dial the device, and click the plus icon.

d. You can add an MCU to the call by clicking the **Add MCU** button, selecting one from the list that appears, and clicking **Add**. If none of the devices that you added to the schedule is capable of hosting the call and you do not add an MCU, a message appears prompting you to add an MCU to facilitate the call. Click **Yes** to add an MCU. When you add a Codian, Radvision, or LifeSize MCU to the call, a **PIN** box appears below the **End date** list box. You can manually enter a PIN (up to 10 characters) for the call or click the grey ring icon that appears in the **PIN** box to automatically generate a 5-digit PIN.

   ***Note:*** Adhoc conferences that use a PIN do not show the PIN in the **Schedule call** dialog box when you view the call details from the **Events** page.

   You can also take advantage of cascading MCUs. For more information about using cascading MCUs, refer to “Using Cascading MCUs” on page 78.

e. You can change call settings for a device that you add to the schedule by clicking the row that the device occupies in the **Selected Devices** list and then clicking **Device settings**. You can change the following call settings:

   - Call Type (the protocol)
   - Bandwidth (auto or choose a bandwidth from the list)
   - Direction of the call (incoming or outgoing)
   - Gateway (if applicable)
   - Mute on connect
   - Do not disturb (if applicable)

f. The name and IP address of each managed participant that appears in **Selected Devices** is a link. Clicking the link opens the **Device details** page for that device to enable you to change configuration settings for that device. For more information about using the **Device details** page, refer to “Viewing and Editing Device Details” on page 51. Avaya Video Conferencing Manager automatically updates the call to reflect or adjust to any changes that you make to device settings that affect the call you are scheduling or editing (for example, changes to the protocols used in the call or the system names). Changes to MCU affinity from the **Device details** page do not affect the call.

6. Click the **Recurrence** button to set up a regularly occurring conference.

   ***Note:*** In an OpenLDAP installation, you cannot schedule calls beyond six months.

7. Click **Call Now** to begin the call immediately or **Schedule Call** to begin the call at the specified time. If the call is not configured properly, an error message appears asking you to configure the call. Click **Configure** for Avaya Video Conferencing Manager to choose a valid configuration for the call.

   ***Note:*** You may encounter a configuration error indicated by an error icon that requires your intervention. For example, you may encounter an error if one of the devices is set to a communication protocol that is incompatible with the protocol settings for other devices in the call. Mouse over the error icon to view a tool tip that describes the error.

   Calls that are successfully scheduled appear on the **Events** page when you choose to display all scheduled events or scheduled calls on the **Display** menu.

## Adding a Device to a Conference

To add a device to a scheduled conference, follow these steps:

1. Click the **Events** button on the navigation bar.
2. Select **Display Scheduled Events** or **Scheduled Calls** from the **Display** list.
3. Right-click the conference to which you want to add a device and click **Edit Details**.

   ***Note:*** If the conference is recurrent, Edit Details appears as **Edit Details - this occurrence** or **Edit Details - this series**.
4. Click **Add device**.
5. Select a device from the list and click **Add** or double-click the device.
6. Close the **Add device** window.
7. Click **Apply changes**.

## Using Cascading MCUs

You can use cascading MCUs to connect calls between two groups of participants. Each groups' communication is channeled through one MCU, and the MCUs pass the bundled communication between each other, greatly reducing the bandwidth needed for the groups to communicate with each other.

For example, eight participants on a network in Japan want to conference with a group of seven participants on a network in Europe. You schedule the 15 participants in a conference along with two MCUs, one that serves the users in Japan, and one that serves the users in Europe. You then drag one of the MCUs (which becomes subservient) and drop it onto the icon for the other (which becomes the master). For this example to work, the MCUs need to know to which participants to connect. You do this by giving the devices affinity to an MCU.

***Note:*** If you created a PIN to use for the call when adding one or more MCUs, the same PIN is used for all cascaded MCUs.

You can assign MCU affinity to a device from the **Devices** page or the **Device details** page of a device. For more information, refer to “Setting or Clearing MCU Affinity” on page 55.

***Note:*** If you are using Microsoft Exchange Server integration with your Avaya Video Conferencing Manager installation, users cannot schedule a cascading MCU call from Microsoft Outlook. You can use cascading MCUs in calls scheduled from Microsoft Outlook by editing the call details from the **Events** page in Avaya Video Conferencing Manager. If you update a call scheduled from Microsoft Outlook by adding cascading MCUs from the **Events** page, Avaya Video Conferencing Manager sends an email to the meeting organizer describing the changes, provided you allow sending email notifications to meeting organizers. For more information about allowing email notifications to be sent to Microsoft Outlook meeting organizers, refer to “Using Avaya Video Conferencing Manager Administrator” on page 88.

## Modifying or Deleting Scheduled Conferences

To modify or delete a scheduled conference, follow these steps:

1. Click the **Events** icon on the navigation bar. The **Events** page appears.
2. On the **Display** menu, click **Display Scheduled Events**.
3. Right-click the event entry for the call you wish to modify or delete and do one of the following:
   - To delete a scheduled conference, right-click the event entry you wish to delete and choose **Delete Schedule**.

     ***Note:*** If Microsoft Exchange Server integration is enabled in Avaya Video Conferencing Manager, you cannot delete a call scheduled through Microsoft Outlook.
   - To edit the entry, click **Edit Details**. The **Schedule Call** dialog box appears.

     ***Note:*** If the event is a recurring event, click either **Edit details for this instance** to modify a single instance of the recurring conference, or click **Edit details for this series** to edit all scheduled occurrences of the conference.

     You can change the type, bandwidth, and direction of a call, remove a participant from the call, alter the date or time, or select a new device to add to the call. You cannot modify events scheduled from Microsoft Outlook in Avaya Video Conferencing Manager, except to add an MCU to a call or to change settings of the scheduled devices.

     When you are finished editing the event, click **Apply Changes**.

## Identifying Conferences Not Scheduled in Avaya Video Conferencing Manager

Calls involving managed devices that were not scheduled through Avaya Video Conferencing Manager appear on the **Events** page with the event name **Adhoc Conference**. Avaya Video Conferencing Manager captures statistics for ad adhoc conferences for reporting purposes.

## Viewing a Call in Progress

You can view a call in progress by completing the following steps:

1. From Avaya Video Conferencing Manager Dashboard, do one of the following:
   - Click **Currently in progress** under **Calls**.
   - Click the **Events** icon in the navigation bar. On the **Events** page, select **Calls in progress** on the **Display** list.
2. Right-click a call and select **Add or Remove Participants**.

   Each participant in the call appears with a series of icons and, for Avaya and LifeSize video communications systems, a snapshot from its camera. Mouse over the icons to learn what each does. With these icons you can do the following:
   - View a calendar of this device's future conferences.
   - Hang up or reconnect to the call.
   - Open call statistics.

     ***Note:*** You can also view call statistics during a call from the **Devices** page by right-clicking a device in a call and clicking **Show call statistics** and from the **Events** page by right-clicking a call in progress and clicking **Show call statistics**.
   - Mute the device.
   - Enable or disable the Do Not Disturb feature on the device (Avaya and LifeSize devices only).
   - Control the volume on the device (Avaya and LifeSize devices only).

## Scheduling Conferences in Microsoft Outlook

If you enabled and configured Microsoft Exchange Server integration with Avaya Video Conferencing Manager, Microsoft Outlook users in your organization can schedule video and voice conferences using a Microsoft Outlook meeting request. Meetings scheduled in Microsoft Outlook with managed audio or video communication systems appear as scheduled calls in Avaya Video Conferencing Manager on the **Events** page. The icon appears in the **Type** column on the **Events** page to indicate an event that is scheduled from Microsoft Outlook. Calls scheduled through Avaya Video Conferencing Manager also appear as events in Microsoft Outlook, thus preventing double booking.

When you schedule an upgrade or template comparison for a managed device in Avaya Video Conferencing Manager, that information is shared with Microsoft Outlook and the device becomes unavailable for scheduling other events.

If none of the devices that the meeting organizer invites to the call is capable of hosting the call, Avaya Video Conferencing Manager automatically adds an available MCU to the schedule and includes the device in the email confirmation that it sends to the meeting organizer.

Cascading MCUs are not available through Microsoft Outlook. If a meeting organizer in Microsoft Outlook includes more participating devices than the host device can connect to, or selects more than one MCU to participate in a call, Avaya Video Conferencing Manager automatically includes only one MCU and makes the selection based on the MCU affinity of the participating devices, if assigned, or the MCU with the greatest number of ports. You can modify a meeting scheduled in Avaya Video Conferencing Manager from Microsoft Outlook to include cascading MCUs only from the Avaya Video Conferencing Manager **Schedule Call** dialog box.

By default, Avaya Video Conferencing Manager automatically places a call scheduled through Microsoft Outlook. If a call fails, Avaya Video Conferencing Manager sends an error email to the meeting organizer indicating that the call failed to launch. To enable the meeting organizer to convert the call to one that is placed manually by the participants, you must enable the feature described in “Specifying a Preferred Method of Participation” on page 83.

***Note:*** Changes made in Avaya Video Conferencing Manager (such as change of MCU, bandwidth, or type of call) to a meeting scheduled through Microsoft Outlook are overwritten by a meeting update that is subsequently sent from Microsoft Outlook.

To schedule a call from Microsoft Outlook, complete the following steps:

1. Create a meeting request in Microsoft Outlook.
2. Add invitees to the request, including the mailboxes for the audio or video communications systems as Required Attendees. Depending on how your administrator configured Avaya Video Conferencing Manager, you may need to add the video or voice communications devices as separate invitees or just the conference rooms in which the devices reside. Consult your Avaya Video Conferencing Manager administrator if you are not sure about which option to choose.

   If you wish to select an MCU to host a multiway call and an MCU is available for scheduling in Microsoft Outlook, add an MCU to the meeting request in the same manner that you add other invitees. Only one MCU is allowed in a call scheduled from Microsoft Outlook. If you choose more than one, Avaya Video Conferencing Manager selects an MCU for you and notifies you of the selection in the confirmation email that it sends when you schedule the call.

If a PIN is required for the call and Avaya Video Conferencing Manager is configured to automatically generate a PIN for calls scheduled with an MCU from Microsoft Outlook, Avaya Video Conferencing Manager sends the PIN to the meeting organizer in the confirmation email when the call is scheduled. The PIN can be modified only in Avaya Video Conferencing Manager. If modified, Avaya Video Conferencing Manager sends an email to the meeting organizer indicating the new PIN. For more information about configuring Avaya Video Conferencing Manager to automatically generate a PIN for calls scheduled from Microsoft Outlook, refer to “Microsoft Exchange Settings” on page 94.

3. Send the meeting request. Avaya Video Conferencing Manager sends an email confirmation regarding the success or failure of the scheduling request. Devices with scheduling conflicts are excluded from the meeting and are noted in the confirmation email.

4. Observe the following rules if you need to update a meeting request:

   a. If you are using webmail for Microsoft Outlook 2003, do not delete all devices from a meeting originally scheduled through Microsoft Outlook. Doing so does not delete the scheduled call in Avaya Video Conferencing Manager. Cancel the meeting instead of deleting all the participating devices if your intent is to cancel the meeting.

   b. If you are using Microsoft Outlook 2007, do not forward a meeting request to devices. Instead, add new devices to the meeting, and send the update to all participants. If you forward a meeting request as a means to add devices to the scheduled call, Avaya Video Conferencing Manager includes only the new devices in the scheduled call and removes all other devices.

   c. If you are using webmail for Microsoft Outlook 2007 when adding or deleting participants to a scheduled call, send the meeting update to all participants when prompted. The default option sends the update only to affected participants which results in Avaya Video Conferencing Manager deleting the original conference participants from the scheduled call.

## Specifying a Preferred Method of Participation

If you enabled and configured Microsoft Exchange Server integration with Avaya Video Conferencing Manager, you can allow human participants in video calls scheduled in Avaya Video Conferencing Manager through Microsoft Outlook to specify a video communications system through which they can be reached. To be included in the scheduled call, the device must be an external device that is not managed by Avaya Video Conferencing Manager. By default, this feature is disabled. Consider enabling this feature if the following conditions exist in your environment:

- Invitees to video meetings in your organization are mobile but have access to video communications systems.
- You wish to allow invitees to video meetings who are external to your organization to include their video communications devices as scheduled participants in calls scheduled through Avaya Video Conferencing Manager.

***Note:*** Support for specifying a preferred device is available only for video devices in this release.

Enabling this feature also allows meeting organizers to convert a call from one that is placed automatically by Avaya Video Conferencing Manager to one that participants place manually.

To enable this feature, select the **Enable participants to select a preferred method of participation** check box on the **Microsoft Exchange Settings** page in Avaya Video Conferencing Manager Administrator.

For more information about Avaya Video Conferencing Manager Administrator, refer to “Using Avaya Video Conferencing Manager Administrator” on page 88.

***Caution:*** Enabling this feature allows a meeting invitee to add an external device to Avaya Video Conferencing Manager’s database without having a user account in Avaya Video Conferencing Manager. Avaya Video Conferencing Manager does not check the validity of the IP address of an external device that is added to a call through this mechanism. When the list of scheduled devices changes due to a reply from a human invitee to the email messages generated by this feature, all human invitees receive an email indicating the change. Avaya recommends that you use this feature in a test environment to ensure that it meets your needs before deploying it in your organization.

When this feature is enabled and a meeting organizer schedules a video call in Avaya Video Conferencing Manager through a meeting invitation in Microsoft Outlook, Avaya Video Conferencing Manager sends a confirmation email to all human participants. The email includes the conference details: the date and start time of the call, the call reservation type, and the IP addresses of the video devices that are scheduled to participate in the call. The email also includes instructions and commands that recipients can use in a reply to the email to do the following:

- Convert a call from one that is placed automatically by Avaya Video Conferencing Manager to one that is placed manually by meeting participants. Only the meeting organizer can reply to the confirmation email with the command `reservation-request` in the body of the reply. By default, Avaya Video Conferencing Manager automatically places a call scheduled through Microsoft Outlook unless it receives this command from the meeting organizer.
- Convert a call from one that is placed manually by meeting participants to one that is placed automatically by Avaya Video Conferencing Manager. Only a meeting organizer can reply to the confirmation email with the command `video-call` in the body of the reply.
- Specify the IP address of an external video communications device through which the invitee wishes to participate in the scheduled call. A meeting invitee can reply to the confirmation email with the command `call@`*`IPaddress`*, where *IPaddress* is the IP address of the external video device to include in the call. Avaya Video Conferencing Manager adds the device to the scheduled call and notifies the meeting organizer and all other human invitees of the change to the list of scheduled devices. If the device does not have an entry in the Avaya Video Conferencing Manager database, Avaya Video Conferencing Manager adds the device as an external device to its database. The device appears as an external device on the **Devices** page. If the device is already a scheduled participant in the call or a managed device, Avaya Video Conferencing Manager ignores the command.

  ***Note:*** Avaya Video Conferencing Manager does not check the validity of the IP address of an external device that is added to a call through this mechanism.
- Remove an external device that an invitee added to the call with the `call@`*`IPaddress`* command. A meeting invitee can reply to the confirmation email with the `busy` command to remove a device that the invitee added to the call in a previous reply to the confirmation email. Avaya Video Conferencing Manager removes the external device from the scheduled call and sends an email to the meeting organizer and all other human invitees of the change to the list of scheduled devices.

The confirmation email sent from Avaya Video Conferencing Manager to participants who are not managed devices indicates the commands available and its usage to the invitees. The following rules must be observed by invitees who wish to reply:

- The confirmation email includes a conference identifier in the body of the message. Invitees who reply must include the conference identifier in the reply.
- The reply must be plain text. Other text formats are not supported in this release.

If the reply email is not in the expected format, Avaya Video Conferencing Manager sends an error email to the invitee with the details of the command. The sender must reply with the correct syntax to the original meeting confirmation email that has the conference identifier (and ensure that the conference identifier is included in the reply), not to the error email.

If the call is in progress when an invitee replies with the `call@`*`IPaddress`* command, Avaya Video Conferencing Manager sends an email to the invitee indicating that the call is in progress and the schedule cannot be modified. Avaya Video Conferencing Manager ignores all other commands sent in a reply if the call is in progress.

Avaya Video Conferencing Manager accepts the `reservation-request` and `video-call` commands from the meeting organizer only and ignores a reply that includes either of these commands if the reply is from any other invitee.

The emails that Avaya Video Conferencing Manager sends to the meeting organizer and to invitees when this feature is enabled are available on the **Microsoft Exchange Settings** page in Avaya Video Conferencing Manager Administrator in the **Email Customization** section. The email identifiers are **Exchange - Schedule created successfully - message to organizer (1)** and **Exchange - Schedule created successfully - message to Invitees (1)**. For more information about Avaya Video Conferencing Manager Administrator, refer to “Using Avaya Video Conferencing Manager Administrator” on page 88.

# Generating Reports

Avaya Video Conferencing Manager provides powerful, graphical report generation capabilities for collected performance data. You can generate data and graphical reports that you can export to PDF or CSV formats. You can also subscribe to a recurring report that is sent to the email address associated with your user account. To view reports, follow these steps:

1. Click the **Reports** button on the navigation bar.
2. Use the hierarchy listing on the left to expand the view.
3. Click the report you want to view.
4. Set the report options and click **Ok**.

   ***Note:*** Use the **Subscribe details** option to set a generation time and the frequency at which the reports are sent to your email. You must have an email address associated with your user account.
5. By default, the report displays as a graph (when available). To view the report as a table, select **Table** in the **View As** options at the top of the **Reports** page.
6. Optionally, to export a report in either PDF or CSV format, select the format from the **Export As** list and then click **Export**. The CSV format is available for selection on the **Export As** list only for report data that appears in a table.

## About Reports

Avaya Video Conferencing Manager includes the following reports.

- **Periodic Reports** show data between specified dates. You can specify a range of dates from which to include data, or choose a particular day, week, month or year. Periodic reports include call statistics (distribution of calls for the selected period), error statistics (distribution of errors over a specific period; error types appear in different colors), and device specific reports (shows activity for a group of devices on the network).
- **Inventory Reports** show information about current devices. Types of inventory reports include hardware audit (listing of hardware types and capabilities) and serial number audit (where devices are located).
- **Summary Reports** show information based on calendar month and year. Types of summary reports include yearly managers summary reports by month or by week.
- **License Audit Reports** show licensed devices by model.
- **Location Audit Reports** show devices by location.
- **ROI Reports** show device utilization by IP address and by model.

- **Codec Reports** show transmit, receive and resolution reports on communications systems.
- **Conference Audit Reports** contain conference-specific statistics.
- **User Reports** show user-specific usage details.
- **Billing Reports** show the estimated cost of calls over a specified date range by device or by location.
- **Diagnostic Reports** represent diagnostic information related to audio and video jitter and packet loss by location or device.
- **Complete CDR data** lists the first 100 call data records for video communications devices. If you choose to export this data, the exported data includes all CDRs.

# Using Avaya Video Conferencing Manager Administrator

Avaya Video Conferencing Manager Administrator is a web-based tool that you can use to view the status of services and modify the following configuration settings for Avaya Video Conferencing Manager:

- application (such as location, system logs, device polling frequency, and the time-out interval for automatic logout)
- alarms
- database management
- billing information
- conferences
- email
- OpenLDAP
- SNMP trap forwarding
- Microsoft Exchange Server integration

To access Avaya Video Conferencing Manager Administrator, click the **Avaya Video Conferencing Manager Administrator** icon on the navigation bar.

## Application Settings

Click **Application Settings** to modify the following Avaya Video Conferencing Manager configuration settings:

- **Location Settings**: Configures the Country, State and IP Address for the Avaya Video Conferencing Manager server. Change the settings by choosing a new one from the appropriate lists.
- **Device Discovery**: Allows you to turn the **DHCP Scan** setting to **ON** or **OFF**. When **DHCP Scan** is **ON**, Avaya Video Conferencing Manager automatically scans for supported devices in subnets in which it currently manages devices.

  For example, if Avaya Video Conferencing Manager manages a device with the IP address 10.95.11.121, DHCP scan, if enabled, scans for supported devices in the IP address range 10.95.11.0 through 10.95.11.255. By default, **DHCP Scan** is **OFF**. Consider enabling DHCP scan when devices do not retain their DHCP assigned address for long periods of time or if devices in the specified IP address range are added to or removed from the network frequently.

- **System Logs**: Avaya recommends that you change the log setting only when directed by Avaya to troubleshoot an issue with Avaya Video Conferencing Manager. The default setting is ERROR. Changing this setting to DEBUG or WARNING may produce large log files.
- **Monitoring**: **Device polling frequency (in minutes)** sets the time interval after which Avaya Video Conferencing Manager polls the status of managed devices. The default is 5 minutes.
- **Automated Logout**: Specifies the length of time, in minutes, after which Avaya Video Conferencing Manager automatically logs off a user due to inactivity. The default is 30 minutes. Specify 0 to disable this feature.

If you change settings on this page, click **Save** for your changes to take effect.

## Alarms Configuration

Click **Alarms Configuration** to modify alarms configuration settings. To determine the status of available alarms, select a type from the **Category** list, and select an alarm ID from the **Alarms** box. The alert message for the alarm appears below the **Alarms** box, and its **Status** is either **ON** or **OFF**.

To assist you in identifying alarms that you may wish to turn off, the category and the alarm ID appear in the email notification that is sent when an alarm is triggered. “Appendix B: Alarms by Category” on page 106 of this guide lists all categories, alarm IDs, and the alert message associated with each alarm. Entries in the alarms **Category** and **Alarms** lists appear in alphabetical order.

If you change the status of any alarm, the **Save** button becomes active. Click **Save** to save your changes.

## Database Management

Backing up the PostgreSQL database used by Avaya Video Conferencing Manager and associated files and being able to restore those files is integral to managing audio and video communications systems with Avaya Video Conferencing Manager. Click **Database Management** to perform these tasks. The current **Database Edition** appears at the top of the page.

### Backing up the Avaya Video Conferencing Manager Database

1. Click **Back up Database** to create a PostgreSQL database back up.

   A file download dialog box appears with the date-stamped .BAK file.

2. Click **Save**.

### Restoring the Avaya Video Conferencing Manager Database from a Backup

Once you have created a copy of your database, you can recover or restore the files if needed in the event of an equipment failure.

1. Click **Browse** and locate the proper .BAK file.
2. Click **Restore Database**.

   ***Caution:*** This process cannot be undone.

## Billing Information

Avaya Video Conferencing Manager uses billing information to estimate the cost of calls placed with your audio and video communications devices. Click **Billing Information** to update the cost per KB by location.

To add or update an entry, select the **Country**, **State** (if applicable), and **Call Type**, and enter the **Cost Per KB**. The **Currency** you choose is used for all entries.

***Note:*** Ensure that the country and state are also configured on the devices that you wish to include in the billing reports. No data appears in billing reports if the country and state are not set on the devices and in Avaya Video Conferencing Manager Administrator.

Click **Add/Update** to save your changes, before you add or update another entry.

To delete an entry, select the **Country**, **State** (if applicable), and **Call Type**, and click **Delete**.

## Conference Settings

Click **Conference Settings** to modify the following configuration settings for calls and conferences:

- **Monitor Call Statistics**: Select this check box to enable Avaya Video Conferencing Manager to compile statistics for managed calls.
- **Show snapshots with call details**: Select this check box to display a snapshot from each participant in a call when viewing a call in progress from the **Events** page.

  ***Note:*** Snapshots are available for managed Avaya and LifeSize devices only.
- **Call Termination Alert Interval**: Enter the time, in minutes, before the end of a call at which time Avaya Video Conferencing Manager will send an alarm and email to the administrator regarding a call's termination. The default is 15 minutes.

- **Call Statistics Monitoring Interval**: Enter the time interval after which call statistics are polled for calls placed with Avaya Video Conferencing Manager.

  ***Note:*** Call statistics monitoring is set to 3 minutes by default. This setting may cause high CPU usage for the `LSCService.exe` process during calls and slow response to tasks performed with the user interface. Depending on the volume of calls and the CPU requirements of other applications running on the server, you may wish to disable **Monitor Call Statistics** or increase the time interval after which Avaya Video Conferencing Manager monitors call statistics.

- **Call Retry Attempts**: Enter the number of times a conference will retry a failed call. The default is 1.

If you change settings on this page, click **Save** for your changes to take effect.

## Email Settings

Click **Email Settings** to modify the following configuration settings for email alerts and messages:

- **SMTP Server**: Enter the address of the SMTP server Avaya Video Conferencing Manager is to use to send emails about alarms. For Microsoft Exchange enabled users, use the email server address you use for Microsoft Exchange Server IP in the Microsoft Exchange Integration page.
- **Email Address**: Enter the addresses of those who are to receive alarms. You can enter multiple addresses separated by commas.
- **From Address**: Enter the address that is to be the source of the email alerts.

If you change settings on this page, click **Save** for your changes to take effect.

## Conference Alert Threshold Settings

Click **Conference Threshold Settings** to modify the following alert threshold settings for audio and video in calls. When Avaya Video Conferencing Manager detects figures above these thresholds, it sends an alert to the email addresses listed as recipients on the **Email Settings** page.

### Audio Settings

Enter the threshold figures for:

- **Transmit Jitter**: Enter a value between 1 and 1000. The default is 40.
- **Receiver Jitter**: Enter a value between 1 and 1000. The default is 40.
- **Transmit Packet Loss %**: Enter a value between 1 and 100. The default is 5.
- **Receive Packet Loss %**: Enter a value between 1 and 100. The default is 5.

**Video Settings**

Enter the threshold figures for:

- **Transmit Jitter**: Enter a value between 1 and 1000. The default is 100.
- **Receiver Jitter**: Enter a value between 1 and 1000. The default is 100.
- **Transmit Packet Loss %**: Enter a value between 1 and 100. The default is 5.
- **Receive Packet Loss %**: Enter a value between 1 and 100. The default is 5.
- **Transmit F/S**: Enter a value between 1 and 60. The default is 7.
- **Receiver F/S**: Enter a value between 1 and 60. The default is 7.

If you change settings on this page, click **Save** for your changes to take effect.

## LDAP Settings

Click **LDAP Settings** to modify the following OpenLDAP configuration settings:

- You can modify the **OpenLDAP server IP Address** or **Port** number. You can also change the **Domain suffix for the OpenLDAP Directory**.
- **User Authentication**: Either **Configure for OpenLDAP** or **Configure for Active Directory** is available, depending on the choice you made during installation of Avaya Video Conferencing Manager.
  - If you chose OpenLDAP, you can change the account password. No other account details can be changed. These fields are for updating the password in Avaya Video Conferencing Manager if you changed it in OpenLDAP.
  - If you chose Active Directory, you can change the user name and password that you specified during installation. The new account must be a domain account with the ability to search the Active Directory.

If you change settings on this page, click **Save** for your changes to take effect.

## Avaya Video Conferencing Manager Diagnostics

Click **Avaya Video Conferencing Manager Diagnostics** to view version information, port status and the status of services used by Avaya Video Conferencing Manager.

To start or stop services listed under **Service Name**, access the machine on which Avaya Video Conferencing Manager is installed and access **Services** from **Administrative Tools** in the **Control Panel**.

**Port Status** lists the status of ports required by Avaya Video Conferencing Manager. When the Avaya Video Conferencing Manager service is stopped, none of these ports should be in use. If one or more are in use, some other application or service is using those ports and may interfere with the proper execution of Avaya Video Conferencing Manager.

## Northbound Settings

Click **Northbound Settings** to enable or disable forwarding of SNMP traps (alarms) and configure trap destinations to which Avaya Video Conferencing Manager forwards traps from all managed video and voice communications devices.

If you configure trap destinations in Avaya Video Conferencing Manager Administrator, Avaya Video Conferencing Manager forwards traps from all managed video and voice communication devices to these destinations. To specify trap destinations for a single device, use the **Northbound** tab on the **Device details** page of the device. For more information, refer to “Forwarding SNMP Traps with Northbound Settings” on page 53.

Select or clear the **Enable Avaya Video Conferencing Manager Northbound Settings** check box and click **Save** to enable or disable SNMP trap forwarding.

***Note:*** By default, SNMP trap forwarding is enabled. Clearing this check box disables SNMP trap forwarding from all managed video and voice communication devices in Avaya Video Conferencing Manager. This also removes access to the **Northbound** tab on the **Device details** page of all devices and disables forwarding traps to any device-specific destinations specified on the **Northbound** tab. If you disable trap forwarding, refresh your browser before accessing the **Device details** page for a managed video or voice communications device.

Follow these steps to add a trap destination for forwarding SNMP traps for all managed video and voice communications devices from Avaya Video Conferencing Manager:

1. In **IP Address**, specify an address to which Avaya Video Conferencing Manager forwards SNMP traps from managed video and voice communication devices.
2. In **Port,** specify the port on the given IP address to which Avaya Video Conferencing Manager forwards the SNMP trap.
3. In **UserName**, specify a user name for authentication on the specified IP address (not to exceed 40 characters).
4. In **Password**, specify a password for authentication on the specified IP address (not to exceed 40 characters).
5. Click **Add**. The IP address you specify appears in the list box.

6. Click **Save** to save your changes.

   ***Note:*** To remove a trap destination, click its IP address in the list box and click **Delete**.

## Microsoft Exchange Settings

If you chose to integrate Avaya Video Conferencing Manager with Microsoft Exchange Server during the Avaya Video Conferencing Manager installation process, you can modify the configuration settings for the integration using Avaya Video Conferencing Manager Administrator. You can also modify the email messages that Avaya Video Conferencing Manager automatically sends to meeting participants. Click **Microsoft Exchange Settings** to change the following Microsoft Exchange Server settings for Avaya Video Conferencing Manager:

- **Enable Microsoft Exchange integration**: Clear or re-select this check box to disable or re-enable this feature. Select the version of Microsoft Exchange Server used in the integration.
- **Require HTTP Access**: Select or clear this check box to either require or not require secure HTTP.
- **Autogenerate PIN for calls scheduled through Microsoft Exchange**: Select this box to automatically generate a PIN for a conference call when a meeting organizer adds an MCU to a meeting request.
- **Enable device management through email**: Enables administrators to manage devices with email commands. For more information about available commands, refer to “Managing a Device Through Email” on page 61.
- **Enable participants to select a preferred method of participation**: Select this check box if you wish to enable meeting invitees to a video conference that is scheduled through Microsoft Outlook to specify an external video device to add to the call. By default, this feature is disabled. Enabling this feature also enables the meeting organizer to specify whether the call should be placed automatically by Avaya Video Conferencing Manager or placed manually by the meeting participants. For more information about this feature, refer to “Specifying a Preferred Method of Participation” on page 83.

  ***Caution:*** Enabling this feature allows a meeting invitee to add an external device to Avaya Video Conferencing Manager’s database without having a user account in Avaya Video Conferencing Manager. Avaya Video Conferencing Manager does not check the validity of the IP address of an external device that is added to a call through this mechanism. When the list of scheduled devices changes due to an email response from a human invitee, all human invitees receive an email indicating the change. Avaya recommends that you use this feature in a test environment to ensure that it meets your needs before deploying it in your organization.

- **Maximum number of days for schedules to be allowed within:** Set the scope of valid conference scheduling in the box.
- **Microsoft Exchange Server IP**: Enter the IP address of the Microsoft Exchange Sever.
- **Microsoft Exchange Server Domain**: Enter the Microsoft Exchange server domain.
- **Microsoft Exchange User**: User name of the Avaya Video Conferencing Manager account in Microsoft Exchange.
- **Avaya Video Conferencing Manager Email**: Enter the email address of the account Avaya Video Conferencing Manager monitors to provide scheduling integration with Microsoft Exchange Server.
- **Password**: Enter a password for the Avaya Video Conferencing Manager Email.

If you change any of these settings, click **Save** for your changes to take effect.

In the **Email Customization** section on this page, you can customize the email messages that Avaya Video Conferencing Manager automatically generates and sends to Microsoft Outlook users. You can also choose whether Avaya Video Conferencing Manager sends any of these messages by selecting or clearing the **Send this email** check box that appears with each message.

> ***Caution:*** Avoid changing any line of text that includes the $ symbol. At minimum, do not delete the $ symbol.

Use the **Reset** button if you need to return the messages to default values.

***Note:*** The email identifiers **Exchange - Schedule created successfully - message to organizer (1)** and **Exchange - Schedule created successfully - message to Invitees (1)** are sent only when the **Enable participants to select a preferred method of participation** check box is selected. For more information about this feature, refer to “Specifying a Preferred Method of Participation” on page 83.

If you change email customization settings, click **Save** for your changes to take effect.

## Troubleshooting Avaya Video Conferencing Manager

If your Avaya Video Conferencing Manager installation or upgrade fails, or you cannot access the user interface after performing an installation or upgrade, use the information in this section to resolve the issue. For all other issues, or if the issue persists, contact Avaya Technical Services for assistance.

## Exporting Page Views

At the top of most pages in Avaya Video Conferencing Manager an option to export the current view as a PDF document appears. This feature is useful for troubleshooting purposes when you are working with Avaya Technical Services representatives.

## Starting and Stopping Avaya Video Conferencing Manager

If you need to stop the Avaya Video Conferencing Manager Server in the Services window on the machine on which Avaya Video Conferencing Manager is installed, use the **Start** option to restart the service. Using the **Restart** option produces an error.

## Maintenance with Microsoft Exchange Server Integration

Once integrated, Avaya Video Conferencing Manager won't run correctly if Microsoft Exchange Server 2007 goes down or is offline. If you must disable Microsoft Exchange 2007 Server, disable Microsoft Exchange integration in Avaya Video Conferencing Manager Administrator first. No conferences scheduled through Microsoft Outlook will be lost.

## Firewall Issues

Avaya Video Conferencing Manager must be able to ping devices on the network. Ensure your firewall is not blocking ping requests. A device's status changes to **Unreachable** if Avaya Video Conferencing Manager cannot ping it.

## Installation Ends with an Error Message

The Avaya Video Conferencing Manager installation program returns an error message and quits if any of the following conditions exist:

- An incompatible version of OpenSSL exists. When you click **OK** in the message dialog box that identifies this condition and then click **Next** in the installation dialog box, the installation program quits. You must then delete the LIBEAY32.dll and SSLEAY32.dll files (located in the C:\windows\system32 folder) and uninstall Avaya Video Conferencing Manager before running the Avaya Video Conferencing Manager installation program again. To uninstall Avaya Video Conferencing Manager, refer to "Removing Avaya Video Conferencing Manager" on page 99.

  ***Caution:*** If you encounter this message during an upgrade, you cannot continue the upgrade or return your existing installation to its previous state without uninstalling Avaya Video Conferencing Manager, reinstalling the previous version and restoring its database from a backup. For more information, refer to "Upgrade Prerequisites" on page 25.

- Data folders from a previous, removed PostgreSQL installation exist and the Avaya Video Conferencing Manager installation program cannot delete them. Delete the folders and then run the Avaya Video Conferencing Manager installation program.
- During a new installation of Avaya Video Conferencing Manager, an installation of OpenLDAP or PostgreSQL already exists. Remove the existing OpenLDAP or PostgreSQL installation and then run the Avaya Video Conferencing Manager installation program.
- Insufficient free disk space exists. Make available at least 500MB of free disk space on the server and then run the Avaya Video Conferencing Manager installation program.
- The upgrade process does not support the current Avaya Video Conferencing Manager installation.

## Status Messages Require Additional Action

During an installation of Avaya Video Conferencing Manager, the following status messages may appear.

| Status Message | Cause and Resolution |
|---|---|
| Could not access VBScript runtime for custom action <*name of custom action*>. | The Windows Scripting Host (WSH) is needed to run a VBScript custom action during the installation, but the WSH is not installed on the target machine.<br>Follow the instructions for downloading and installing Microsoft Windows Script 5.6 at:<br>`http://www.microsoft.com/downloads/details.aspx?familyid=C717D943-7E4B-4622-86EB-95A22B832CAA&displaylang=en` |
| Failed to update Avaya Video Conferencing Manager database with LDAP information. | Configuration of the LDAP database failed due to errors encountered during the installation of the database. |
| The process cannot access the file <*path and file name of OpenLDAP file*> because it is being used by another process. | This message may appear after you click **Configure LDAP** during the installation process.<br>Access **Start->Control Panel->Administrative Tools->Services** and stop the OpenLDAP Directory Service. Continue the installation by clicking **Configure LDAP**. |

## Web Sites in IIS Function Improperly After an Upgrade

During an upgrade, the Avaya Video Conferencing Manager installation program changes the ASP.NET version of all web sites installed in IIS to v2.0. Other web sites installed in IIS that are not running in their own application pools and that rely on an earlier version of Microsoft .NET Framework may function improperly after the upgrade. To work around this issue, do the following after performing the upgrade:

1. Open the IIS Manager. Click **Start->Programs->Administrative Tools->IIS Manager**.
2. Expand **Web Sites->Default Web Site**.
3. For each web application under **Default Web Site**, right-click the application and select **Properties**.
4. Click the **ASP.NET** tab. Ensure that the version is set to the appropriate Framework version for the application. For Avaya Video Conferencing Manager, the version is 2.0.

## Device Status Not Updating

Device status may fail to update dynamically in the user interface if other services or applications are listening on ports 161 or 162. Ensure that only Avaya Video Conferencing Manager is listening on these ports. For more information about ports, refer to “Ports” on page 17.

## Login Issues

If the Avaya Video Conferencing Manager launch page does not appear when you attempt to access the user interface, do the following on the computer on which Avaya Video Conferencing Manager is installed:

- Access **Start->Control Panel->Administrative Tools->Services** and ensure that the status of the IIS Admin service is Started. If you installed Avaya Video Conferencing Manager by upgrading from a previous version, do the following:
  1. Go to **Start->Run**. The **Run** dialog box appears.
  2. Type `iisreset` in the **Open** list box.
  3. Click **OK**.
- Access Avaya Video Conferencing Manager Administrator.
  - Click **Service Status & Ports** and ensure that the status of all services listed in the **Services Name** column is Running.

- Click **LDAP Settings**. Ensure that the IP address that you selected for the OpenLDAP server in step 4 on page 23 is correct. If it is not, click **Configure**. The **LDAP Settings** dialog box appears. Select the correct IP address and click **Save**.

If you are still unable to connect to the web server, you may need to reassign the server certificate to correct the problem. Complete the following steps:

1. Access **Start->Run**, enter `inetmgr`, and press **Enter**.
2. Expand the tree to expose the **Default Web Site** node.
3. Right-click the **Default Web Site** node and click **Properties**.
4. Click the **Directory Security** tab and click **Server Certificate**.
5. Click **Next**.
6. Select the **Assign an existing certificate** option and click **Next**.
7. Select the certificate displayed in the selection box and click **Next**.
8. Select the default SSL port and click **Next**.
9. Click **Next** and click **Finish**.
10. Select **Start->Run**, enter `inetmgr`, and press **Enter**. The IIS web server restarts and you should be able to access the Avaya Video Conferencing Manager web page using https.

## Removing Avaya Video Conferencing Manager

The Avaya Video Conferencing Manager uninstall program removes all components that Avaya Video Conferencing Manager installed, except the installation directory, any log files and device upgrade files that are stored in the installation directory, and the PostgreSQL directory. You must remove these directories manually after removing Avaya Video Conferencing Manager.

***Note:*** This release of Avaya Video Conferencing Manager does not appear in the **Add or Remove Programs** window.

To remove Avaya Video Conferencing Manager from the server, follow these steps:

1. Access **Start->All Programs->Avaya ->Video Conferencing Manager->Uninstall**.
2. When prompted to remove Avaya Video Conferencing Manager, click **Yes**.
3. When prompted to remove PostgreSQL, select **Remove** and click **Yes**.
4. When prompted to remove OpenLDAP, click **Yes**.

5. On the **Start** menu, click **Run**. The **Run** dialog box appears.
6. Enter `inetmgr` in the **Open** list box.
7. Expand the tree to expose the **Default Web Site** node.
8. Remove `AvayaAuraVideoSystemManager`.
9. In the **Default Web Site** directory, remove `AvayaAura.aspx`
10. Right click **Default Web Site** node, and then click **Properties**.
11. Click the **Documents** tab and remove `AvayaAura.aspx` from the list of files.
12. Restart your computer to ensure that the changes take effect.

# Appendix A: User Role Access

The following table describes the scope of access to functionality in Avaya Video Conferencing Manager for each user role.

| Page Name | Functionality | Administrator | Engineer | Operator |
|---|---|---|---|---|
| **Alarms** | View | Yes | Yes | Yes |
| | Acknowledge | Yes | Yes | No |
| | Own | Yes | Yes | No |
| | Acknowledge with resolution | Yes | Yes | No |
| | Forward | Yes | Yes | No |
| | Assign | Yes | No | No |
| | Export All or Selected as CSV or XML | Yes | No | No |
| **Devices** | View lists of devices | Yes | Yes | Yes |
| | View device details | Yes | Yes | Yes |
| | Launch device browser interface | Yes | Yes | Yes |
| | Schedule a call | Yes | Yes | Yes |
| | Join device to a conference | Yes | Yes | Yes |
| | View call statistics | Yes | Yes | Yes |
| | View device calendar | Yes | Yes | Yes |

| Page Name | Functionality | Administrator | Engineer | Operator |
|---|---|---|---|---|
| **Devices** (continued) | Set MCU Affinity | Yes | Yes | No |
| | Update license | Yes | Yes | No |
| | Register email address to device | Yes | Yes | No |
| | Register gatekeeper | Yes | Yes | No |
| | Send a message to a device | Yes | Yes | Yes |
| | Discover devices | Yes | Yes | No |
| | Add a new device | Yes | Yes | No |
| | Refresh all | Yes | Yes | No |
| | Update password | Yes | Yes | No |
| | Change password | Yes | Yes | No |
| | View alarms | Yes | Yes | No |
| | Refresh device | Yes | Yes | No |
| | Schedule upgrade | Yes | Yes | No |
| | Reboot device | Yes | Yes | No |
| | Delete device | Yes | Yes | No |
| | Take device offline | Yes | No | No |
| | Update device name in list entry | Yes | No | No |

| Page Name | Functionality | Administrator | Engineer | Operator |
|---|---|---|---|---|
| **Devices** (continued) | Update device IP in list entry | Yes | No | No |
| | Modify device details | Yes | No | No |
| | Manage devices | Yes | No | No |
| | Create templates | Yes | No | No |
| **Events** | View events | Yes | Yes | Yes |
| | Schedule calls | Yes | Yes | Yes |
| | Add or remove participants to a call | Yes | Yes | Yes |
| | Drop a call | Yes | Yes | Yes |
| | Redial completed calls | Yes | Yes | Yes |
| | View call details | Yes | Yes | Yes |
| | Show call statistics | Yes | Yes | Yes |
| | View system calendar | Yes | Yes | Yes |
| | Schedule device upgrades | Yes | Yes | No |
| | Delete scheduled calls | Yes | Yes | No |
| | Delete scheduled upgrades | Yes | Yes | No |

| Page Name | Functionality | Administrator | Engineer | Operator |
|---|---|---|---|---|
| **Events** (continued) | Schedule template events | Yes | No | No |
| | Delete scheduled template events | Yes | No | No |
| | Schedule device offline | Yes | No | No |
| **Reports** | Generate all reports | Yes | Yes | Yes |
| **Templates** | Create templates | Yes | No | No |
| | Back up or restore a device | Yes | No | No |
| | View logs | Yes | No | No |
| **Packages** | View list | Yes | Yes | Yes |
| | Upload | Yes | Yes | No |
| | Delete | Yes | Yes | No |
| **Password** | Specify default passwords for devices and protocols | Yes | No | No |
| **User Management** | View user lists | Yes | Yes (LDAP only) | Yes (LDAP only) |
| | Modify user details | Yes | Yes (LDAP only and only for logged in user) | Yes (LDAP only and only for logged in user) |
| | Import/add new user | Yes | No | No |
| | Delete user | Yes | No | No |

| Page Name | Functionality | Administrator | Engineer | Operator |
|---|---|---|---|---|
| **Help** | Access help for using Avaya Video Conferencing Manager | Yes | Yes | Yes |
| **Avaya Video Conferencing Manager Administrator** | Access Avaya Video Conferencing Manager Administrator | Yes | No | No |
| **Not applicable. Feature available when Microsoft Exchange integration is enabled.** | Manage devices through email commands | Yes | No | No |

# Appendix B: Alarms by Category

## authentication

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_LOGIN_FAIL | Invalid username or password. | OFF |

## call-stats

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_CALL_STATS_HIGH_JITTER | Audio or video jitter has exceeded the configured threshold value. | ON |
| ID_CALL_STATS_POOR_FPS | Frames per second has fallen below the configured threshold value. | ON |
| ID_CUMULATIVE_PKT_LOSS_AUDIO | Cumulative packet loss exceeded the configured threshold value. | ON |
| ID_CUMULATIVE_PKT_LOSS_VIDEO | Cumulative packet loss exceeded the configured threshold value. | ON |

## Codian

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_CODIAN_AUTH_FAILURE | Authentication failure | ON |
| ID_CODIAN_LINK_DOWN | Link down. | ON |
| ID_CODIAN_TRAP_REC_CONFIG_MODIFIED | Trap receiver configurations were modified. | ON |

## conference

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_ABNORMAL_CALL_TERMINATION | Abnormal termination of the conference. | ON |
| ID_CALL_PENDING_TERMINATION | Conference $1$ is pending termination. | ON |
| ID_CONF_CANNOT_EXTEND_NEXT_CALL_READY | The conference cannot be extended since the calling station has already been scheduled to participate in another conference during the requested time period. | ON |
| ID_CONF_DELETED_FROM_CONF_TBL | Deleted conference $1$ from the conference table. | ON |
| ID_CONF_DEV_BUSY_AT_SCHEDULED_TIME | One or more devices added to this conference are busy for the scheduled time. | ON |
| ID_CONF_EXT_FAILED_DB_ERROR | Failed to extend the conference $1$. A database error occurred. | ON |
| ID_CONF_EXT_FAILED_DEV_NOT_LS | Failed to extend conference $1$. The calling station is not an Avaya device. | ON |
| ID_CONF_EXT_FAILED_NEXT_CALL_SCHEDULED | Failed to extend the conference $1$. The calling station has already been scheduled to participate in another conference during the requested time period. | ON |

## conference (Continued)

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_CONF_EXTEND_FAILED_INVALID_DEV_STATUS | Failed to extend conference $1$. Invalid device status. | ON |
| ID_CONF_EXTENED | Extended conference $1$. | ON |
| ID_CONF_EXTENSION_FAILURE_1 | Failed to extend the conference $1$. | ON |
| ID_CONF_EXTENSION_NOT_PREFERRED | The user decided not to extend the conference. | ON |
| ID_CONF_EXTENSION_STOPPED_BY_USER | The user decided not to extend the conference $1$. | ON |
| ID_CONF_EXTERNAL_EP_UNAVAILABLE | One of the external participants in the conference $1$ is not available. | ON |
| ID_CONF_FAILED_EMPTY_DEV_LIST | Failed to launch conference $1$. Empty device list. | ON |
| ID_CONF_HAS_BEEN_TERMINATED_ALREADY | The conference has already been terminated. | ON |
| ID_CONF_LAUNCH_FAIL_1_DB_ERR | Failed to launch the conference $1$. A database error occurred. | ON |
| ID_CONF_LAUNCH_FAIL_DB_ERROR_OCCURED | Failed to launch conference $1$. A database error occurred. | ON |
| ID_CONF_LAUNCH_FAIL_INSUFFICIENT_DEV | Failed to launch conference $1$. Not enough devices are running. | ON |

## conference (Continued)

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_CONF_LAUNCH_FAILED_NO_DEV | Failed to launch conference $1$. No managed devices found. | ON |
| ID_CONF_SAVE_FAIL_DB_ERROR | Failed to save conference $1$. A database error occurred. | ON |
| ID_CONF_SAVE_FAIL_SW_UPGRADE_CONFLICT | Failed to save conference $1$. | ON |
| ID_CONF_SAVE_FAILED | Failed to save conference $1$. No managed devices were found. | ON |
| ID_CONF_SAVE_FAILED_DUE_TO_CONFIG_SCHEDULES | Failed to save conference $1$. An error occurred when checking for conflicts with configuration management schedules. | ON |
| ID_CONF_SAVE_SUCCESS | Conference $1$ was saved successfully. | ON |
| ID_CONF_STATUS_UPDATE_FAILED | Unable to update the status of the conference $1$ to failed. A database error occurred. | ON |
| ID_CONF_STATUS_UPDATE_FAILED_DB_ERR | Unable to update the status of the conference $1$ to failed. A database error occurred. | ON |
| ID_CONF_TERMINATION_PENDING | Call has exceeded its scheduled duration. | ON |

## conference (Continued)

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_DEL_CONF_FAILED_CONF_LAUNCHED | Failed to delete the conference $1$ from the conference table. The conference has already been dialed or terminated. | ON |
| ID_DEL_CONF_FAILED_DB_ERROR | Failed to delete conference $1$ from the conference table; a database error occurred. | ON |
| ID_DEL_CONF_FAILED_DB_ERROR_1 | Failed to delete the conference from the conference table; a database error occurred. | ON |
| ID_DEL_CONF_FAILED_DB_ERROR_UPDATE_FAIL | Failed to delete conferences from the conference table. A database error occurred. | ON |
| ID_DEL_CONF_FAILED_NO_MATCH_FOUND | Failed to delete the conference $1$ from the conference table. No matching conference was found. | ON |
| ID_ERR_ON_CHECKING_CONFLICT_FOR_UPG | An error occurred when checking for conflicts with the software upgrade schedules. | ON |
| ID_ERR_ON_CHECKING_CONFLICT_WITH_CONFIG_SYS | An error occurred when checking for conflicts with the configuration management schedules. | ON |
| ID_FAILED_CONF_LAUNCH_NOW | Failed to launch the conference. | ON |

## conference (Continued)

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_FAILED_CONF_TERMINATION | Failed to terminate the conference. | ON |
| ID_FAILED_TO_FIND_CALL_STATION | Failed to launch conference $1$. Unable to find a calling station to dial the conference. | ON |
| ID_FAILED_UPDATE_CONF_STATUS_TO_TERMINATED | Failed to update the status of the conference $1$ to terminated. | ON |
| ID_IMPROPER_CONF_TERMINATION | Improper termination: $1$. | ON |
| ID_NO_MANAGED_DEV_SELECTED_FOR_CONF | No managed devices are selected. | ON |
| ID_NO_MATCHING_CONF_FOUND | No matching conference found. | ON |
| ID_PARTICIPANT_ADDITION_FAILED | Participant addition failed. | ON |
| ID_PARTICIPANT_DEV_REMOVE_FAILED | Failed to remove participant device $1$ from the conference $2$. | ON |
| ID_PARTICIPANT_DEV_REMOVED | Participant device $1$ was removed from the conference $2$. | ON |
| ID_TERMINATE_FAILED_FOR_CALLS_FROM_IP | $1$ : Unable to terminate calls made by this device. | ON |
| ID_UNABLE_TO_FIND_CALLING_STATION | Unable to find a calling station to launch the conference. | ON |
| ID_UNABLE_TO_MAKE_CALLS | Unable to make a call to $1$ from $2$. | ON |

## conference (Continued)

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_UNABLE_TO_MAKE_CALLS_NO_SERVICE_PREFIX | Unable to make a call to $1$ from $2$. MCU does not have any valid service prefix. | ON |
| ID_UNABLE_TO_UPDATE_CONF_TO_INPROGRESS | Unable to update the status of the conference $1$. A database error occurred. | ON |

## ftp

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_FTP_DEV_DOWNLOAD_FAILED | Could not download the files from the device using FTP. | ON |
| ID_FTP_FAILED | FTP authentication failed | ON |
| ID_FTP_SESSION_OPEN_FAILED | Failed to open a FTP session on the device. | ON |
| ID_FTP_UPLOAD_FAILED | Could not upload the file to the device using FTP. | ON |

## http

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_CHECK_HHTP_SETTINGS | The device could not be contacted through HTTP. | ON |

## ldap

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_COUNTRY_STATE_INFO_MODIFY_FAILED | Failed to modify the country/state information in LDAP | ON |
| ID_DEV_ADDED_TO_LDAP | The device was added successfully to LDAP. | ON |
| ID_DEV_INFO_MODIFIED_IN_LDAP | Device information was modified successfully in LDAP. | ON |
| ID_FAILED_TO_MODIFY_DEV_INFO_IN_LDAP | Failed to modify the device information in LDAP. | ON |
| ID_LDAP_ADD_FAIL_DUPLICATE_ENTRY | Failed to add the device to LDAP. A duplicate entry exists. | ON |
| ID_LDAP_ADD_FAIL_DUPLICATE_IP | Failed to add the device to LDAP. Duplicate IP address. | ON |
| ID_LDAP_CONNECT_ERROR | Unable to connect to the server. | ON |
| ID_LDAP_MODIFY_FAILED_FOR_DUPLICATE_IP | LDAP modification failed due to a duplicate device IP. | ON |

## Avaya

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_LSC_ALL_PRI_PORTS_DOWN | All PRI ports are down. | ON |
| ID_LSC_BOOT_COMPLETE | Boot complete. | ON |
| ID_LSC_BOOT_FAIL | Boot failed. | ON |

## Avaya (Continued)

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_LSC_CALL_CONNEC | Call connected | ON |
| ID_LSC_CALL_CONNECTED | Call connected. | ON |
| ID_LSC_CALL_DISCONNEC | Call disconnected. | ON |
| ID_LSC_CALL_DISCONNECTED | Call disconnected. | ON |
| ID_LSC_CH_CONN | Channel connected. | ON |
| ID_LSC_CH_DISONN | Channel disconnected. | ON |
| ID_LSC_CHANGE_IN_PRI_PORT_STATUS | The PRI port status changed. | ON |
| ID_LSC_CHANNEL_CONNECTED | Channel connected. | ON |
| ID_LSC_CHANNEL_DISCONNECTED | Channel disconnected. | ON |
| ID_LSC_CONF_TERMINATED | Conference terminated. | OFF |
| ID_LSC_DEV_DOWN_TRAP | Device down trap. | ON |
| ID_LSC_DEV_UP_TRAP | Device up trap. | ON |
| ID_LSC_DIALING_MULTIP_CALL | Dialing a multipoint call. | ON |
| ID_LSC_DIALING_P2P_CALL | Dialing a two way call. | ON |
| ID_LSC_DOWNGRADE_FINISHED | Downgrade finished. | ON |
| ID_LSC_DOWNGRADE_STARTED | Downgrade started. | ON |
| ID_LSC_ENDPOINT_MAKING_CALL | Device is placing a call. | ON |
| ID_LSC_ENTER_UPG_MODE | Entering upgrade mode. | ON |

## Avaya (Continued)

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_LSC_INCOMING_CALL | Device received a call. | ON |
| ID_LSC_ISDN_LINE_DOWN | ISDN line down. | ON |
| ID_LSC_ISDN_LINE_ERR | Error with ISDN line. | ON |
| ID_LSC_ISDN_LINE_UP | ISDN line up. | ON |
| ID_LSC_PEI_BRI_CABLE_IN | A BRI cable is plugged in. | ON |
| ID_LSC_PEI_BRI_CABLE_OUT | A BRI cable is unplugged. | ON |
| ID_LSC_PRI_PORT_DOWN | PRI port is down. | ON |
| ID_LSC_PRIPORT_UP | The PRI port is up. | ON |
| ID_LSC_SYS_ALARM | *This alarm is deprecated. Setting the status has no effect.* | ON |
| ID_LSC_SYS_ERROR | System encountered an error. | ON |
| ID_LSC_SYS_EVENT | *This alarm is deprecated. Setting the status has no effect.* | ON |
| ID_LSC_SYSTEM_HEAT_STATUS_NORMAL | System heat status is back to normal. | ON |
| ID_LSC_SYSTEM_HEAT_STATUS_WARNING | System heat status is abnormal. | ON |
| ID_LSC_SYSTEM_HEAT_STATUS_OVERHEATED | System is overheated. | ON |
| ID_LSC_UPG_FINISHED | Upgrade finished. | ON |
| ID_LSC_UPG_STARTED | Upgrade started. | ON |
| ID_LSC_UPGR_FINISHED | *This alarm is deprecated. Setting the status has no effect.* | ON |

## Avaya (Continued)

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_LSC_V35_UP | *This alarm is deprecated. Setting the status has no effect.* | OFF |

## Avaya Video Conferencing Manager

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_ADD_USER | $1$ $2$ has been added. | ON |
| ID_ALARM_EMAIL_INFO | *This alarm is deprecated. Setting the status has no effect.* | ON |
| ID_BACKUP_HISTORY_ALARMS_TO_PATH | Back up history alarms to $1$. | ON |
| ID_CALL_STATS_ALARM | A call statistics threshold violation has occurred. | ON |
| ID_CHECK_FILENAME_VALIDITY | Check if filenames are valid and the device is running. | ON |
| ID_CLISSHKEY_APPLY_FAILED | Failed to apply ssh key. | ON |
| ID_CMD_VALIDATION_FAILED | Failed to validate the command. | ON |
| ID_CONFIG_CANCELLED | *This alarm is deprecated. Setting the status has no effect.* | ON |
| ID_DATABASE_BACKED_UP | Database backup to file $1$ successful at $2$. | ON |

## Avaya Video Conferencing Manager (Continued)

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_DEV_INFO_MODIFY_FAILURE_IN_EXCHG | Failed to modify the device information in the Microsoft Exchange Server. | ON |
| ID_DELETE_USER | $1$ $2$ has been deleted. | ON |
| ID_DEV_INFO_UPDATED_IN_EXCHG_SRVR | Device information updated successfully in the Microsoft Exchange Server. | ON |
| ID_DEV_MAC_NULL | The MAC address of the device is null. | ON |
| ID_DEV_STATUS_INAPPROPRIATE_FOR_DEL | Device deletion failed. Device status is not appropriate for deletion. | ON |
| ID_DEVICE_DELETED_FROM_INVENTORY | Device deleted from device inventory. | ON |
| ID_DEVICE_DOWN | The device is not running. | ON |
| ID_DEVICE_UP | The device is running. | ON |
| ID_DIR_CREATE_FAIL | Failed to create the required directory structure. | ON |
| ID_DIR_NOT_NULL | Failed to upload files. Directory name cannot be empty. | ON |
| ID_EXPORT_HISTORY_COMPLETE | Exported the history alarms table to “$1$”. | ON |
| ID_FAILED_ADD_TO_EXCHG | Failed to add the device to the Microsoft Exchange Server. | ON |

## Avaya Video Conferencing Manager (Continued)

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_FAILED_DEV_REBOOT | Failed to reboot the device. | ON |
| ID_FAILED_DEVICE_DEL_FROM_ADDR_BOOK | Failed to delete device from address book. | ON |
| ID_FAILED_TO_BACKUP_HISTORY | Failed to backup history alarms. | ON |
| ID_FAILED_TO_EXPORT_HISTORY | Failed to export history alarms. | ON |
| ID_FILE_NOT_FOUND | File not found. | ON |
| ID_FILE_UPLOAD_FAILED | Failed to upload files. Filename cannot be empty. | ON |
| ID_FILENAME_NOT_FOUND | Failed to upload files. Requested filename not found. | ON |
| ID_HISTORY_BACKUP_HISTROY_ALARMS_EXCEED | The alarms in history exceed the critical limit. | ON |
| ID_HISTORY_CRITICAL_LIMIT_EXCEED | The alarms in history exceed the critical limit. | ON |
| ID_HISTORY_EXPORT_SUCCESS | Successfully exported the history alarms table. | ON |
| ID_HISTORY_HIGHER_LIMIT_EXCEED | The alarms in history exceed the higher limit. | ON |
| ID_HISTORY_LOW_LIMIT_EXCEED | The alarms in history exceed the lower limit. | ON |
| ID_LOW_LICENSE_COUNT | Available licenses remaining are less than 15% of the total licenses. | ON |

## Avaya Video Conferencing Manager (Continued)

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_LSC_SERVER_SHUTDOWN | Attempting to shut down the Avaya Video Conferencing Manager server at $1$. | ON |
| ID_LSC_SERVER_SHUTDOWN_FAILED | Avaya Video Conferencing Manager server shutdown failed at $1$. | ON |
| ID_LSC_SERVER_STARTUP | Avaya Video Conferencing Manager server started at $1$ by $2$. | ON |
| ID_MIB_LOAD_FAILED | Failed to load the MIB files. Check for MIB files. | ON |
| ID_MODIFY_ALARM_SW_UPGRADE_PACK | Failed to modify conference $1$. Error when checking for conflicts with software upgrade schedules. | ON |
| ID_MODIFY_CONF_DB_ERROR | Failed to modify conference $1$. Database error. | ON |
| ID_MODIFY_CONF_FAIL_LAUNCHED_OR_TERMINATED | Failed to modify conference $1$. Conference has already been launched or terminated. | ON |
| ID_MODIFY_CONF_FAIL_NO_MGMD_DEV | Failed to modify conference $1$. No managed devices found. | ON |
| ID_MODIFY_CONF_MODULE_SETTINGS_ERR | Failed to modify conference $1$. Error when checking for conflicts with configuration management schedules. | ON |

## Avaya Video Conferencing Manager (Continued)

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_MODIFY_CONF_NO_MATCH | Failed to modify conference $1$. No matching conference found. | ON |
| ID_MODIFY_CONF_NO_MATCH_1 | Failed to modify conference. No matching conference found. | ON |
| ID_MODIFY_USER | $1$ $2$ has been modified. | ON |
| ID_NO_FILES_DOWNLOAD | No files to download. | ON |
| ID_NO_MORE_LICENSES | No licenses left. | ON |
| ID_PARAM_KEY_UNAVAILABLE | *This alarm is deprecated. Setting the status has no effect.* | ON |
| ID_REFRESH_FAIL_FOR_ALL_DEV_PARAM | Refresh failed. Failure in retrieving all device parameters. | ON |
| ID_REFRESH_FAIL_FOR_COMMON_DEV_PARAM | Refresh failed. Failure in retrieving common device parameters. | ON |
| ID_SERVER_CONNECT_ERROR | Unable to connect to the server. | ON |
| ID_SOFTWARE_UPGRADE_STARTED | Software upgrade started. | ON |
| ID_START_APPLYING_TEMPLATE | Applying template. | ON |
| ID_UNABLE_TO_ACCESS_DB | The database could not be accessed or a SQL string was incorrect. | ON |

## Avaya Video Conferencing Manager (Continued)

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_UNKNOWN_ERROR | An unknown error has occurred. | ON |
| ID_UPDATE_PWD_ON_DEV_FAILED | Failed to update the password on the device. | ON |
| ID_USER_FAILED_TO_LOGIN | User $1$ failed to log in. | ON |
| ID_USER_NOT_REGISTERED | You are not registered with Avaya Video Conferencing Manager. | ON |
| ID_USR_PWD_PAIR_FAIL | Username/password pair failed on the device. | ON |

## Polycom

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_DEV_INFO_UPDATE_SUCCESS_FOR_POLYCOM | Device information uploaded successfully to all Polycom devices. | ON |
| ID_POLYCOM_AUTH_FAILURE | Authentication failure. | ON |
| ID_POLYCOM_AUTO_ANS_CHANGE | Auto answer change. | ON |
| ID_POLYCOM_BATTERY_LOW | Low battery. | ON |
| ID_POLYCOM_CALL_DOWN | Call terminated. | ON |
| ID_POLYCOM_CALL_FAILED | Call failed. | ON |
| ID_POLYCOM_CALL_UP | Call is in progress. | ON |

## Polycom (Continued)

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_POLYCOM_GDS_DOWN | *This alarm is deprecated. Setting the status has no effect.* | ON |
| ID_POLYCOM_GDS_OFF | *This alarm is deprecated. Setting the status has no effect.* | ON |
| ID_POLYCOM_GDS_UP | *This alarm is deprecated. Setting the status has no effect.* | ON |
| ID_POLYCOM_INTF_TYPE_CHANGE | The interface type changed. | ON |
| ID_POLYCOM_IP_ADDR_CHANGE | The IP address changed. | ON |
| ID_POLYCOM_JITTER_EXCESSIVE | Jitter is excessive. | ON |
| ID_POLYCOM_LATENCY_EXSS | Latency is excessive. | ON |
| ID_POLYCOM_LINE_DISABLED | Line disabled. | ON |
| ID_POLYCOM_LINE_DOWN | Line down. | ON |
| ID_POLYCOM_LINE_ENABLED | Line enabled. | ON |
| ID_POLYCOM_LINE_UP | Line up. | ON |
| ID_POLYCOM_LINK_DOWN | Link down. | ON |
| ID_POLYCOM_LINK_UP | Link up. | ON |
| ID_POLYCOM_LOGIN_FAILED | Login failed. | ON |
| ID_POLYCOM_LOGIN_OK | Login OK. | ON |
| ID_POLYCOM_MAIN_CAM_DOWN | Main camera is not running. | ON |

## Polycom (Continued)

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_POLYCOM_MAIN_CAM_UP | Main camera is running. | ON |
| ID_POLYCOM_MIC_CHANGE | Microphone change. | ON |
| ID_POLYCOM_PERCENT_PACK_LOSS_EXSS | Percentage of packet loss is excessive. | ON |
| ID_POLYCOM_TIME_SERVER_DOWN | Time server is not running. | ON |
| ID_POLYCOM_TIME_SERVER_OFF | Time server is off. | ON |
| ID_POLYCOM_TIME_SERVER_ON | Time server is on. | ON |
| ID_POLYCOM_TIME_SERVER_UP | Time server is running. | ON |
| ID_POLYCOM_USER_ASSIST | *This alarm is deprecated. Setting the status has no effect.* | ON |
| ID_POLYCOM_V35_PORTS_ENABLED | v.35 ports enabled. | ON |
| ID_POLYCOM_VISUAL_CONCERT_UP | Visual Concert is running. | ON |
| ID_POLYCOM_VISUAL_CONCERT_OFF | Visual Concert is off. | ON |

## software upgrade

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_SW_UPGRADE_CANCELLED_NOW | The upgrade could not occur since the device is currently not reachable. | ON |
| ID_SW_UPGRADE_FAILED | The software upgrade failed. | ON |

## software upgrade (Continued)

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_SW_UPGRADE_FAILED_LOGIN | The software upgrade failed because of a login failure. | ON |
| ID_SW_UPGRADE_FAILED_PACKAGE_NOT_FOUND | The software upgrade failed because the file $1$ does not exist. | ON |
| ID_SW_UPGRADE_FINISHED | The software upgrade has finished. The device will reboot. | ON |
| ID_SW_UPGRADE_START | The software upgrade has started. | ON |

## SNMP

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_SNMP_FAILED | The device could not be contacted through SNMP. | ON |
| ID_SNMP_SEND_FAILED | Could not send the SNMP request to the requested device. | ON |
| ID_SNMP_TRAP_SETTING_FAILED | Setting SNMP trap destinations failed on the device after discovery. | ON |

## ssh

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_SSH_SESSION_FAILED | Failed to open an SSH session on the device. | ON |

## Tandberg

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_TANDBERG_AUTH_FAIL | Authentication failure. | ON |
| ID_TANDBERG_CALL_MODE_CHANGE | Call mode change. | ON |
| ID_TANDBERG_COLD_START | *This alarm is deprecated. Setting the status has no effect.* | ON |
| ID_TANDBERG_DISCONNECT | *This alarm is deprecated. Setting the status has no effect.* | ON |
| ID_TANDBERG_FINISHED_UPGRADE | Upgrade finished. | ON |
| ID_TANDBERG_IP_AUTH_FAIL | IP authentication failure. | ON |
| ID_TANDBERG_LINK_DOWN | Link down. | ON |
| ID_TANDBERG_LINK_UP | Link up. | ON |
| ID_TANDBERG_LOW_BATTERY | Low battery. | ON |
| ID_TANDBERG_LOW_SPEEDING | Down speeding. | ON |
| ID_TANDBERG_START_UPGRADE | Start upgrade. | ON |
| ID_TANDBERG_WARM_START | *This alarm is deprecated. Setting the status has no effect.* | ON |

## telnet

| Alarm ID | Description | Default Status |
|---|---|---|
| ID_TELNET_FAILED | Telnet authentication failed for the specified password. | ON |
| ID_TELNET_SESSION_FAILED | Could not open a Telnet session on the device. | ON |
| ID_TELNET_SESSION_LOST | Cannot execute the command on the device since the Telnet session to the requested device is lost. | ON |